ASSA ABLOY

Aperio® Programming Application Manual

Document No: ST-001321-E, Issue date: 1 August 2014

aperio™

The global leader in
door opening solutions

Table of Contents

1 Introduction

Purpose

The main purpose of this manual is to provide information for installation and configuration of Aperio Online/Offline based products using the Aperio Programming Application.

The manual is intended for installation personnel, project managers and people with similar responsibilities.

Scope

This manual includes a complete description of all functionality and settings in the Aperio Programming Application.

For quick installation instructions of a standard Aperio online system including communication hubs and locks/sensors. Refer to ref [2], Aperio Online Quick Installation Guide. For a standard Offline system, refer to ref [3], Aperio Offline Quick Installation Guide.

This manual is applicable to version 2.6.6 of the Aperio Programming Application.

Applicable Products

This manual can be used for all versions of communication hubs.

Aperio support in the EAC system

Note that the Aperio support may vary depending on the Aperio communication hub used and the level of integration. Please contact your OEM for details.

Abbreviations and Definitions

Abbreviation	Definition
EAC	Electronic Access Control. The system controlling the access rules which is then conveyed to user cards through the Offline Updater.
DIP	Dual in-line Package. A manual electric switch used for settings on the communication hub.
RFID	Radio Frequency Identification. The credential technology used.
ACU	Access Control Unit. The device within the EAC system that communicates with the communication hub.
TLS	Transport Layer Security. Cryptographic protocol that provides secure communication over TCP/IP connections.
SOAA	Standard Offline Access Application. A standardized way of exchanging access data between credential and offline lock.
V2	Generation 2 of the Aperio platform.
V2SE	Generation 2 of the Aperio platform using HID SE.
V3	Generation 3 of the Aperio platform

References

[1]	ST-001323-Aperio Online Mechanical Installation Manual
[2]	ST-001322-Aperio Online Quick Installation Guide
[3]	ST-001802-Aperio Offline Quick Installation Guide

2 System Overview

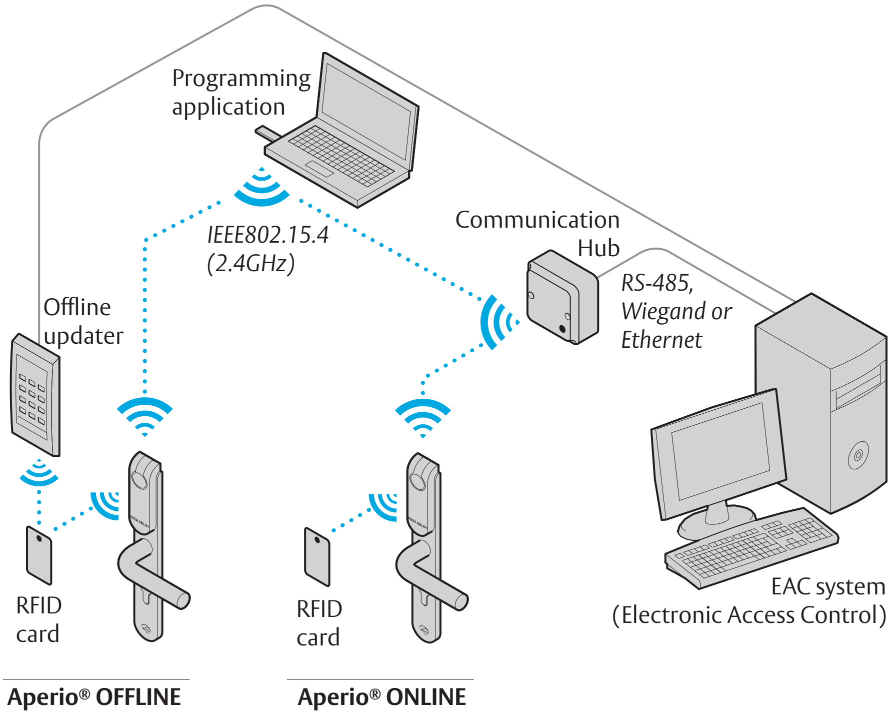


Figure 1.
Aperio technology overview

The Aperio system

The Aperio system is used in the following way: The user holds an RFID credential in front of an online or offline lock.

- **Aperio Online:** An online lock sends card credentials wirelessly to the communication hub which in turn communicates with an EAC (Electronic Access Control) system (wired through RS-485, Wiegand or TCP/IP). The EAC system makes the access decision. The decision is sent via the communication hub to the lock and access is granted or denied.
- **Aperio Offline:** Access decision is taken locally by lock. Result of decision depends on access rights stored on the card and also on lock configuration received from the EAC through offline updaters with setup- or user cards.

Regulatory and security information

See section *"7 Regulatory Information Regarding the Aperio USB Radio Dongle" on page 108.*

The Aperio programming application

The Programming Application is used for the configuration of a door installation. It is normally installed on a laptop and is used with an Aperio USB radio dongle connected to one of the USB ports.

The USB radio dongle enables the programming application to connect to a communication hub and an online lock (via the communication hub) or directly to an offline lock.

Communication hub versions and EAC interface

There are four communication hub types according to the table below:

Version	Interface	Maximum number of locks/sensors
AH15	Wiegand/RS 485*	1
AH20	Wiegand	1
AH30	RS-485	8
AH40	IP (Ethernet)	8

* The firmware type loaded into the communication hub controls what interface is enabled.

3 The Programming Application Overview

About the Programming Application

- Software running under 32-bit or 64-bit versions of Windows 7, Windows 8, Vista or XP.
- Multi-language installation management tool.
- Encrypted installation database.

Refer to section "*6 Installation of Programming Application and USB Radio dongle firmware" on page 107* for installation and upgrade from earlier versions.

Information of encryption key

To obtain secure communication between communication hubs and locks/sensors an Encryption key is used. This Encryption key should be handled with the same care as the Master Key in a traditional Master Key System. A person with access to the Encryption key can gain unauthorized access to any Aperio door in the system. Once loaded into the Programming Application, it will be stored encrypted in a local database and any copy should be erased from the hard drive or e-mail. It is however recommended that a copy of the encryption key is stored in safe.

The encryption key file is delivered from your local ASSA ABLOY company and should be requested on a customer/site basis.

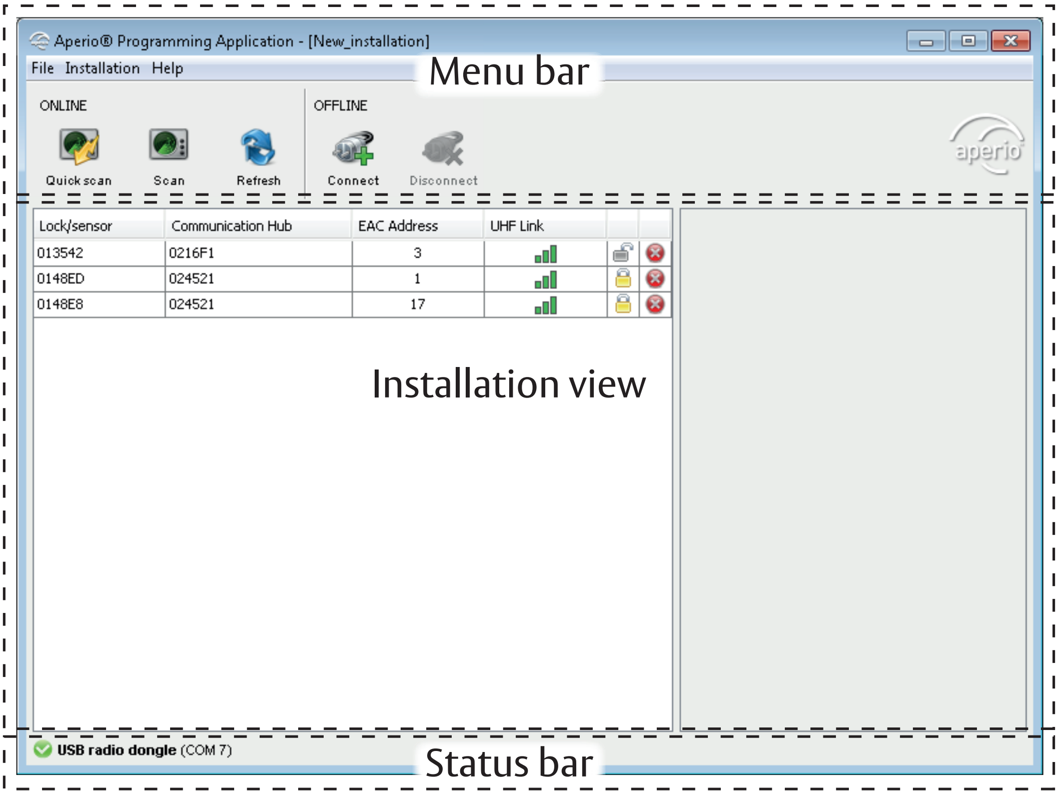
Proper handling of encryption keys is essential to lock/sensor security!

It is absolutely necessary to use the customer encryption key by setting all communication hubs and locks/sensors in Customer mode to ensure a secure and encrypted communication with the lock/sensor.

Main view

The main view of the Programming Application consists of three areas:

- Menu bar: The buttons are used to connect to either Aperio Online communication hubs or Offline locks.
- Installation view: Displays the Aperio devices in the installation.
- Status bar: Information of USB radio dongle connection.



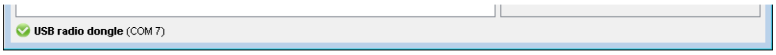
Lock/sensor	Communication Hub	EAC Address	UHF Link		
013542	0216F1	3			
0148ED	024521	1			
0148E8	024521	17			

USB radio dongle (COM 7)

Status bar

The status bar contains the following information:

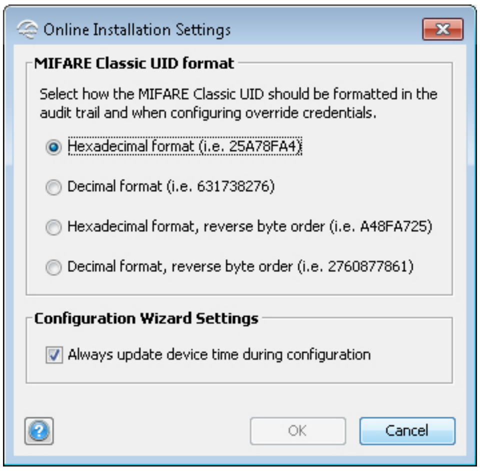
- USB Radio indication



USB radio dongle (COM 7)

Online Installation settings

The *Online Installation Settings* contains settings that are applicable to the current installation. In the menu bar, select *Installation - OnlineSettings...*



MIFARE Classic UID format

Select how the MIFARE Classic UID should be formatted in the audit trail and when configuring override credentials.

- ● Hexadecimal format (i.e. 25A78FA4)
- ○ Decimal format (i.e. 631738276)
- ○ Hexadecimal format, reverse byte order (i.e. A48FA725)
- ○ Decimal format, reverse byte order (i.e. 2760877861)

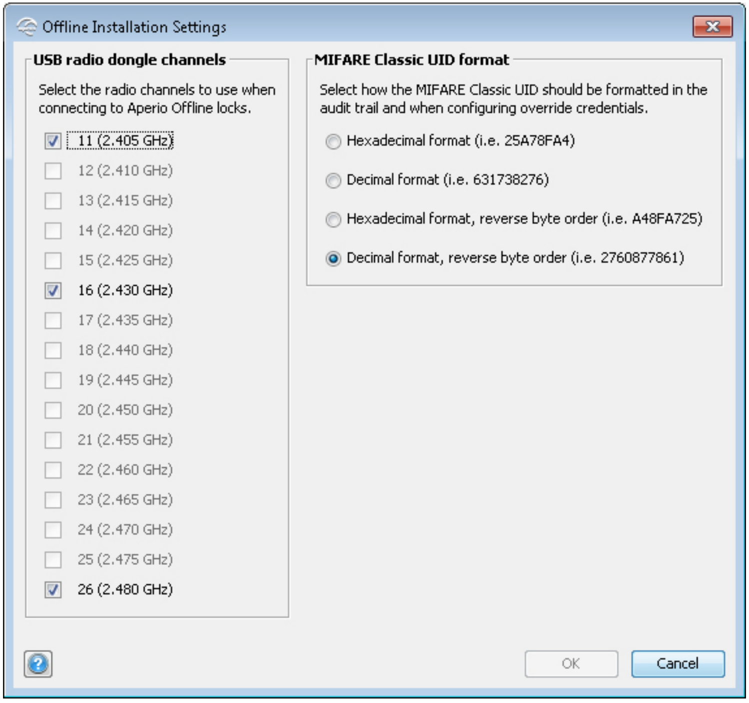
Configuration Wizard Settings

☑ Always update device time during configuration

- **MIFARE Classic UID format:** Selected format will be used for displaying MIFARE Classic Credentials (for example in the Audit trail and Override credential dialogs).
- **Configuration wizard settings:** Select if the lock/sensor should be updated with correct time during configuration.

Offline Installation Settings

The *Offline Installation Settings* contains settings that are applicable to the current installation. In the menu bar, select *Installation - Offline - Settings...*:



USB radio dongle channels

Select the radio channels to use when connecting to Aperio Offline locks.

- ☑ 11 (2.405 GHz)
- □ 12 (2.410 GHz)
- □ 13 (2.415 GHz)
- □ 14 (2.420 GHz)
- □ 15 (2.425 GHz)
- ☑ 16 (2.430 GHz)
- □ 17 (2.435 GHz)
- □ 18 (2.440 GHz)
- □ 19 (2.445 GHz)
- □ 20 (2.450 GHz)
- □ 21 (2.455 GHz)
- □ 22 (2.460 GHz)
- □ 23 (2.465 GHz)
- □ 24 (2.470 GHz)
- □ 25 (2.475 GHz)
- ☑ 26 (2.480 GHz)

MIFARE Classic UID format

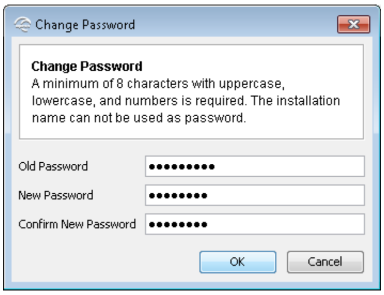
Select how the MIFARE Classic UID should be formatted in the audit trail and when configuring override credentials.

- ○ Hexadecimal format (i.e. 25A78FA4)
- ○ Decimal format (i.e. 631738276)
- ○ Hexadecimal format, reverse byte order (i.e. A48FA725)
- ● Decimal format, reverse byte order (i.e. 2760877861)

- **USB radio channels:** The radio channels that will be used when connecting to the lock.
- **MIFARE Classic UID format:** Selected format will be used for displaying MIFARE Classic, MIFARE Plus and ISO14443-B credentials (for example in the Audit trail).

Change Password

To change password for the current installation, select *Installation - Change Password...* in the menu bar:



Change Password

Change Password
A minimum of 8 characters with uppercase, lowercase, and numbers is required. The installation name can not be used as password.

Old Password ●●●●●●●●●

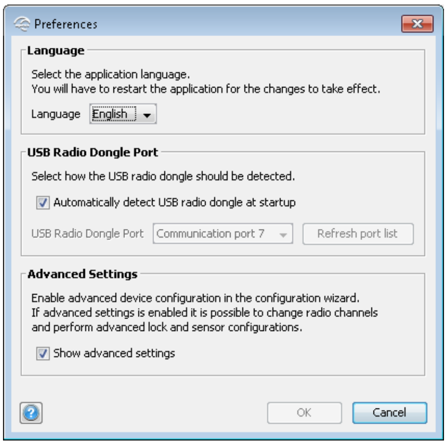
New Password ●●●●●●●●

Confirm New Password ●●●●●●●●

The password must contain at least 8 characters of which at least one upper and lower case character and a number. The installation name can not be used as password.

Preferences

The preferences dialog contains settings that are applicable to all the installations. In the menu bar, select *File - Preferences...*:



Preferences

Language
Select the application language.
You will have to restart the application for the changes to take effect.

Language English

USB Radio Dongle Port
Select how the USB radio dongle should be detected.

☑ Automatically detect USB radio dongle at startup

USB Radio Dongle Port Communication port 7

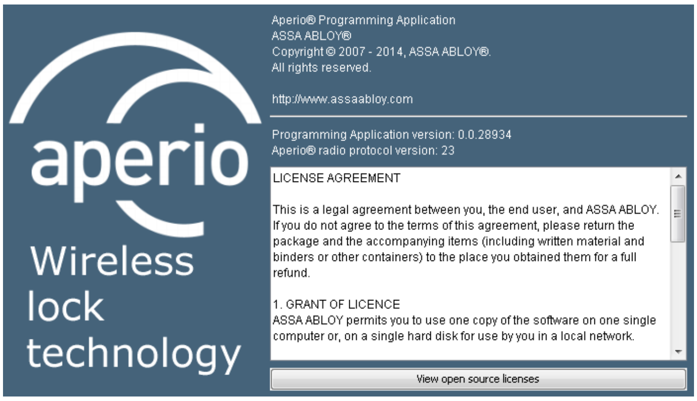
Advanced Settings
Enable advanced device configuration in the configuration wizard.
If advanced settings is enabled it is possible to change radio channels and perform advanced lock and sensor configurations.

☑ Show advanced settings

- **Language:** Select the language used by the Programming Application. For the language changes to take effect, restart the Programming Application.
- **USB Radio Dongle Port:** Automatically detects USB radio at start up: Uncheck this option to manually specify the port used by the USB Radio Dongle, in case of hardware conflict.
- **Advanced settings:** Check this box if you need to perform advanced hub and lock configurations: keypad configuration, advanced settings (changing the radio channel) and advanced lock settings (such as Locking parameters).

Software version

To check the version of installed software, select *About Aperio Programming Application* on the Help menu. Click *View open source licenses* to see related licence information:



Aperio® Programming Application
ASSA ABLOY®
Copyright © 2007 - 2014, ASSA ABLOY®.
All rights reserved.

http://www.assaabloy.com

Programming Application version: 0.0.28934
Aperio® radio protocol version: 23

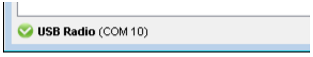
LICENSE AGREEMENT

This is a legal agreement between you, the end user, and ASSA ABLOY. If you do not agree to the terms of this agreement, please return the package and the accompanying items (including written material and binders or other containers) to the place you obtained them for a full refund.

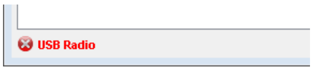
1. GRANT OF LICENCE
ASSA ABLOY permits you to use one copy of the software on one single computer or, on a single hard disk for use by you in a local network.

USB radio indication

USB Radio together with a green check mark indicates that the serial port used is ok and the radio dongle is ready to transmit data.

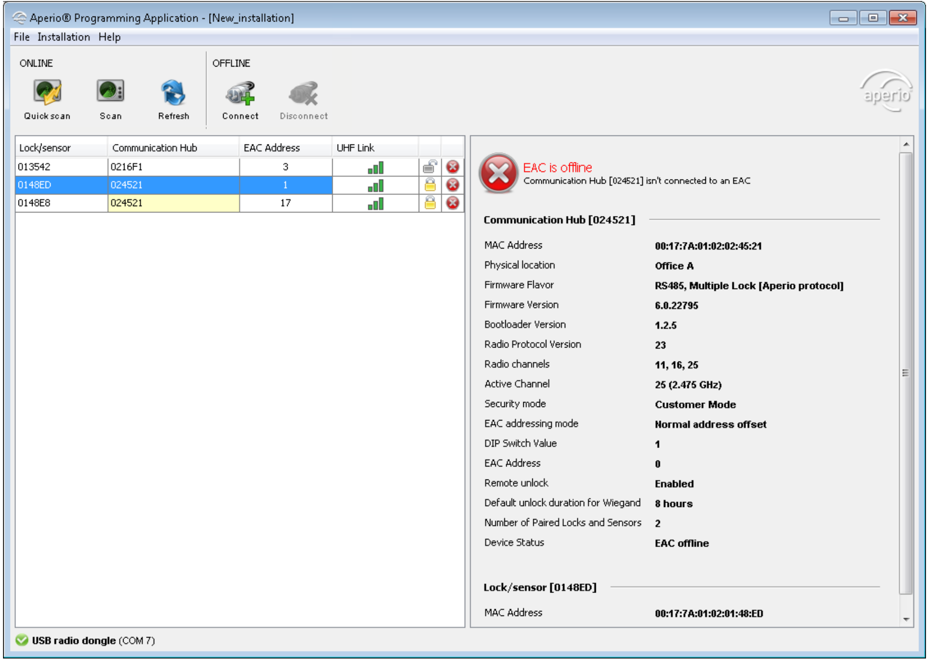

✓ **USB Radio** (COM 10)

USB Radio together with a red cross indicates that the serial port or the USB radio dongle is not ok. (Refer to section "*Preferences*" *on page* 9 to verify that correct settings are used.)


⊗ **USB Radio**

Installation View overview for Aperio Online

The installation view is the main window when working with door installations. This window is automatically displayed after logging in to an installation and after going through the scanning process.



Lock/sensor	Communication Hub	EAC Address	UHF Link		
013542	0216F1	3	▂▄▆	🔓	⊗
0148ED	024521	1	▂▄▆	🔒	⊗
0148E8	024521	17	▂▄▆	🔒	⊗

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

MAC Address	**00:17:7A:01:02:02:45:21**
Physical location	**Office A**
Firmware Flavor	**RS485, Multiple Lock [Aperio protocol]**
Firmware Version	**6.0.22795**
Bootloader Version	**1.2.5**
Radio Protocol Version	**23**
Radio channels	**11, 16, 25**
Active Channel	**25 (2.475 GHz)**
Security mode	**Customer Mode**
EAC addressing mode	**Normal address offset**
DIP Switch Value	**1**
EAC Address	**0**
Remote unlock	**Enabled**
Default unlock duration for Wiegand	**8 hours**
Number of Paired Locks and Sensors	**2**
Device Status	**EAC offline**

Lock/sensor [0148ED]

MAC Address	**00:17:7A:01:02:01:48:ED**

✓ **USB radio dongle** (COM 7)

The following information is shown:

- **Lock/sensor:** Indicates if there is a lock/sensor paired with the communication hub. If there is a paired lock/sensor the MAC address of the lock/sensor is shown.
- **Communication hub:** The MAC address of the communication hub.
- **EAC Address:** Shows the EAC address for the lock paired with this communication hub.
- **UHF Link:** Indicates the strength of the UHF wireless link (through the USB Radio dongle) between the communication hub and the Aperio Programming Application.
  Green: Good
  Yellow: OK
  Red: Not OK (firmware upgrade not allowed)
- **Security Mode:** Indicates the security mode of the communication hub. During final installation all locks and hubs must be changed from Manufacturer mode to Customer mode.

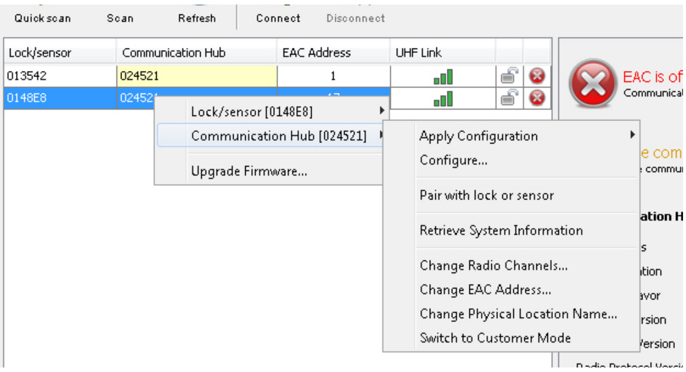
🔒	*Customer mode*	Lock is using secure radio communication with the customer encryption key.
🔓	*Manufacturer mode*	Lock is using insecure radio communication with the default encryption key.

- **Warning indications:** The following warning levels are given. Hoover with the mouse to see more information.

ℹ	For example: Security mode for communication hub is undefined.
ℹ	For example: The communication hub firmware version (Aperio radio protocol version) is older than Aperio Programming Application.
⚠	For example: The Aperio Programming Application is older than the communication hub firmware version (Aperio radio protocol version).
⊗	For example: The security modes in communication hub and lock are not equal and should be changed.

- Detailed information of selected hub and lock/sensor is shown on the right side of the window.

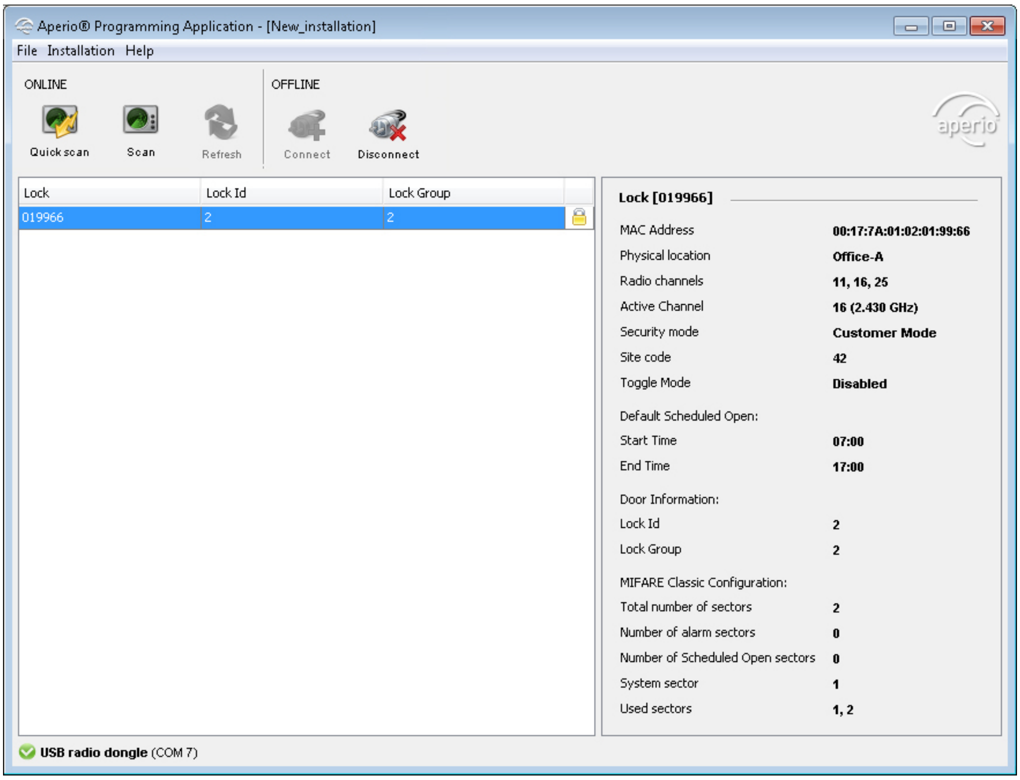
Right-clicking a communication hub or lock/sensor will give access to the functions available in the Programming Application. See section *"4 Programming Application Online Functions" on page 13* for an overview of all functions.



Lock/sensor	Communication Hub	EAC Address	UHF Link		
013542	024521	1		🔓	⊗
0148E8	02452	1		🔓	⊗

Installation View overview for Aperio Offline

The installation view is the main window when working with door installations. This window is displayed after logging in to an installation and after connecting to a lock.



Lock	Lock Id	Lock Group
019966	2	2

Lock [019966]

MAC Address	00:17:7A:01:02:01:99:66
Physical location	Office-A
Radio channels	11, 16, 25
Active Channel	16 (2.430 GHz)
Security mode	Customer Mode
Site code	42
Toggle Mode	Disabled
Default Scheduled Open:	
Start Time	07:00
End Time	17:00
Door Information:	
Lock Id	2
Lock Group	2
MIFARE Classic Configuration:	
Total number of sectors	2
Number of alarm sectors	0
Number of Scheduled Open sectors	0
System sector	1
Used sectors	1, 2

The following information is shown:

- **Lock:** The MAC address of the lock.
- **Lock Id:** The lock id is a unique identification number assigned to the lock.
- **Lock Group:** Lock group is a number used for managing access rights for the lock. Several locks can have the same lock group number.
- **Security Mode:** Indicates the security mode of the communication hub. During final installation all locks must be changed from Manufacturer mode to Customer mode.

🔒	*Customer mode*	Lock is using secure radio communication with the customer encryption key.
🔓	*Manufacturer mode*	Lock is using insecure radio communication with the default encryption key.

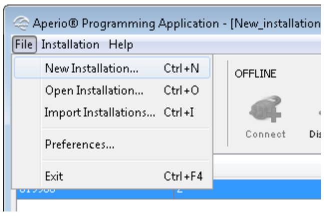
4 Programming Application Online Functions

Opening/creating installations

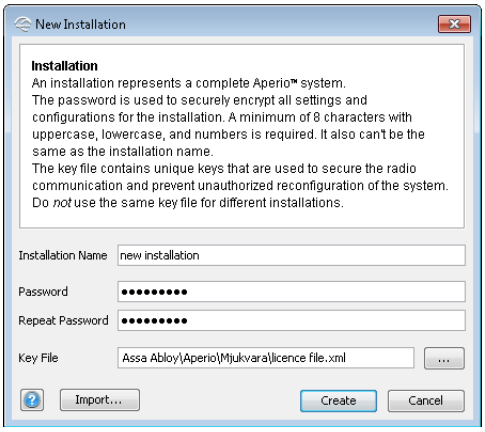
An installation is a password protected set of settings you need when you want to communicate with a hub and/or a lock. An installation is linked to an encryption file that is needed for the communication to work. (The encryption key file is provided by your local ASSA ABLOY company via encrypted e-mail or on a USB memory stick.)

1) Insert the USB Radio dongle and start the Aperio Programming application.

2) Select *File - New installation...* or *Open Installation...* in the Programming Application.


Aperio® Programming Application - [New_installation
File
Installation
Help
New Installation... Ctrl+N
Open Installation... Ctrl+O
Import Installations... Ctrl+I
Preferences...
Exit Ctrl+F4
OFFLINE
Connect

3) For a new installation, enter a name for the installation, a password matching the requirements and finally click the button in the Key file field to load the Encryption key (in XML-format).



Installation
An installation represents a complete Aperio™ system.
The password is used to securely encrypt all settings and configurations for the installation. A minimum of 8 characters with uppercase, lowercase, and numbers is required. It also can't be the same as the installation name.
The key file contains unique keys that are used to secure the radio communication and prevent unauthorized reconfiguration of the system. Do *not* use the same key file for different installations.

Installation Name: new installation

Password: •••••••••

Repeat Password: •••••••••

Key File: Assa Abloy\Aperio\Mjukvara\licence file.xml

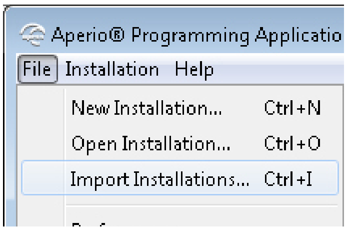
Proper handling of encryption keys is essential to lock/sensor security!

It is absolutely necessary to use the customer encryption key by setting all communication hubs and locks/sensors in Customer mode to ensure a secure and encrypted communication with the lock/sensor.

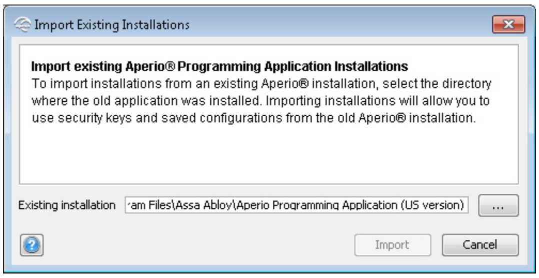
4) Click *Create*.

Import Existing Installations

1) To import an existing Aperio installation including security keys and configurations, select *File-Import Installations...*


Aperio® Programming Applicatio
File Installation Help
New Installation... Ctrl+N
Open Installation... Ctrl+O
Import Installations... Ctrl+I

2) Select the location by clicking the button. Your current installations will not be deleted.

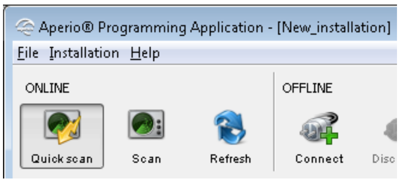

Import Existing Installations

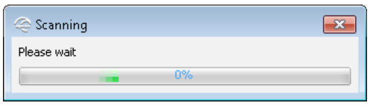
Import existing Aperio® Programming Application Installations
To import installations from an existing Aperio® installation, select the directory where the old application was installed. Importing installations will allow you to use security keys and saved configurations from the old Aperio® installation.

Existing installation ‹am Files\Assa Abloy\Aperio Programming Application (US version)

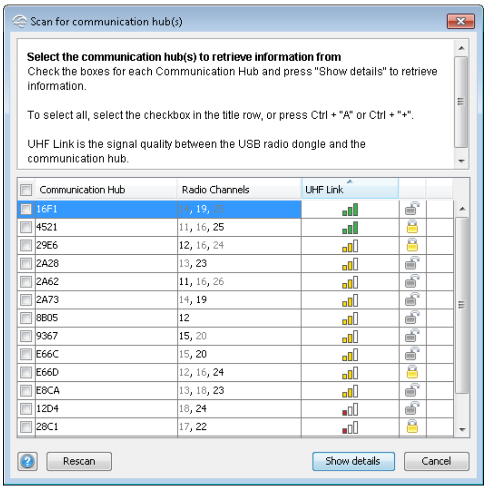
Scanning and adding communication hubs

1) To scan for communication hubs, click *Quick Scan (F7)*. (If your communication hub is not found, retry and click *Scan (Ctrl+F7)*, to perform a more extensive scan.)





Result: All communication hubs within reach of the USB Radio dongle of your computer are displayed in the scan result table.


Scan for communication hub(s)

Select the communication hub(s) to retrieve information from
Check the boxes for each Communication Hub and press "Show details" to retrieve information.

To select all, select the checkbox in the title row, or press Ctrl + "A" or Ctrl + "+".

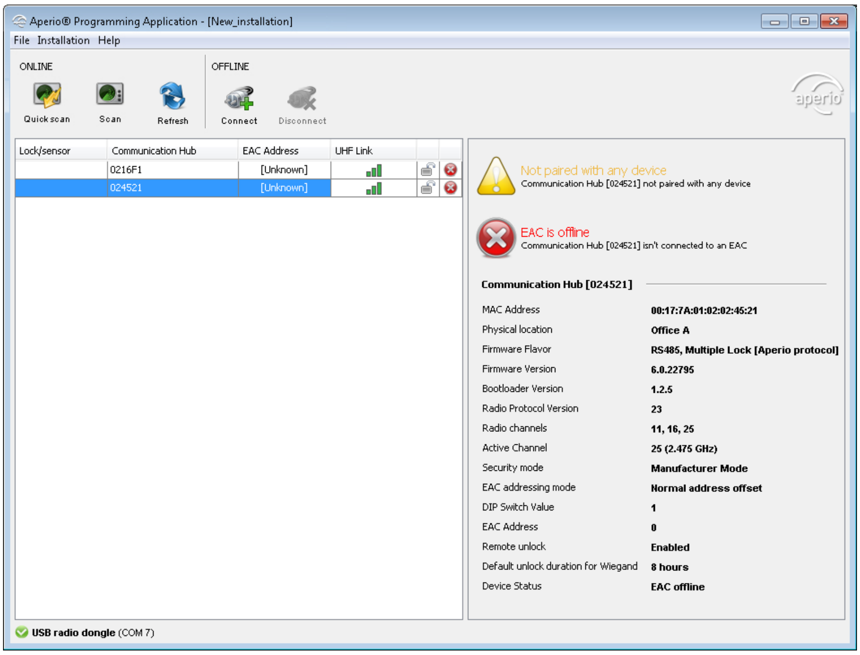
UHF Link is the signal quality between the USB radio dongle and the communication hub.

□ Communication Hub	Radio Channels	UHF Link	
□ 16F1	14, 19, 25	▂▄▆	🔓
□ 4521	11, 16, 25	▂▄▆	🔒
□ 29E6	12, 16, 24	▂▄	🔒
□ 2A28	13, 23	▂▄	🔓
□ 2A62	11, 16, 26	▂▄	🔓
□ 2A73	14, 19	▂▄	🔓
□ 8B05	12	▂▄	🔓
□ 9367	15, 20	▂▄	🔓
□ E66C	15, 20	▂▄	🔓
□ E66D	12, 16, 24	▂▄	🔒
□ E8CA	13, 18, 23	▂▄	🔓
□ 12D4	18, 24	▂	🔓
□ 28C1	17, 22	▂	🔒

2) Locate a communication hub by the last four characters of the communication hub MAC address (ex. 01CF) in the scan result table. The same characters should be on a label on the cover of the communication hub. Click *Rescan* if the communication hubs that you want to configure are not shown in the list.

3) Select the communication hub(s) that you want to include in your installation. Click *Show details* in the window above to view detailed information.

Result: Selected communication hub(s) are displayed in the installation view.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
	024521	[Unknown]	

Not paired with any device
Communication Hub [024521] not paired with any device

EAC is offline
Communication Hub [024521] isn't connected to an EAC

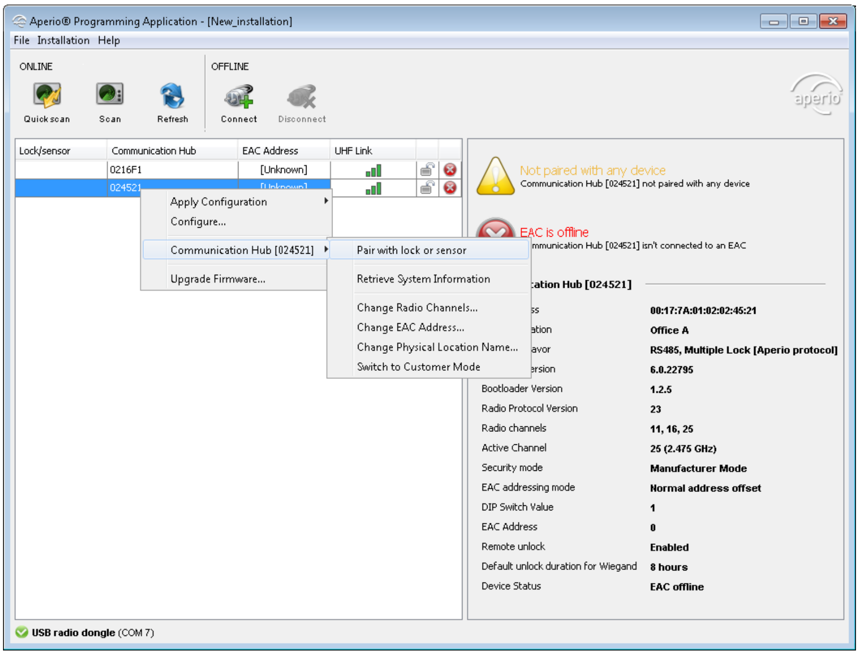
Communication Hub [024521]

MAC Address	00:17:7A:01:02:02:45:21
Physical location	Office A
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.0.22795
Bootloader Version	1.2.5
Radio Protocol Version	23
Radio channels	11, 16, 25
Active Channel	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Device Status	EAC offline

Pairing locks/sensors with communication hub

AH30/AH40 version of the communication hub can be paired with a combination of up to 8 locks/sensors. AH15/AH20 can manage one lock/sensor.

1) Right-click and select *Communication hub - Pair with lock or sensor*.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
	024521	[Unknown]	

Not paired with any device
Communication Hub [024521] not paired with any device

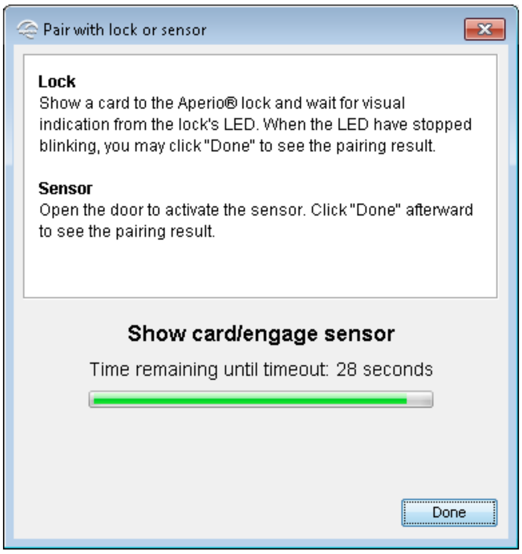
EAC is offline
mmunication Hub [024521] isn't connected to an EAC

ation Hub [024521]

ss	00:17:7A:01:02:02:45:21
ation	Office A
avor	RS485, Multiple Lock [Aperio protocol]
ersion	6.0.22795
Bootloader Version	1.2.5
Radio Protocol Version	23
Radio channels	11, 16, 25
Active Channel	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Device Status	EAC offline

✓ USB radio dongle (COM 7)

2) The pairing process starts. Hold the credential at the lock, or engage the magnet for the sensor to pair the hardware with the communication hub.



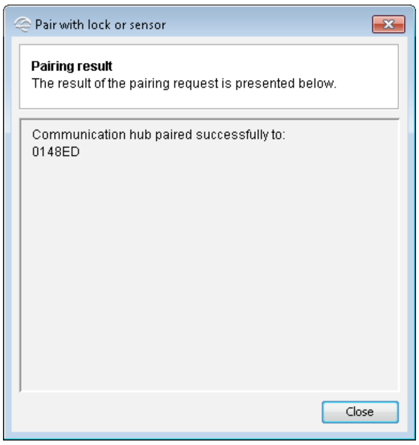
Lock
Show a card to the Aperio® lock and wait for visual indication from the lock's LED. When the LED have stopped blinking, you may click "Done" to see the pairing result.

Sensor
Open the door to activate the sensor. Click "Done" afterward to see the pairing result.

Show card/engage sensor

Time remaining until timeout: 28 seconds

3) When the lock has stopped blinking or when the LED on the communication hub turns green, you can click *Done* to see the pairing result.
   Result: The result is displayed.

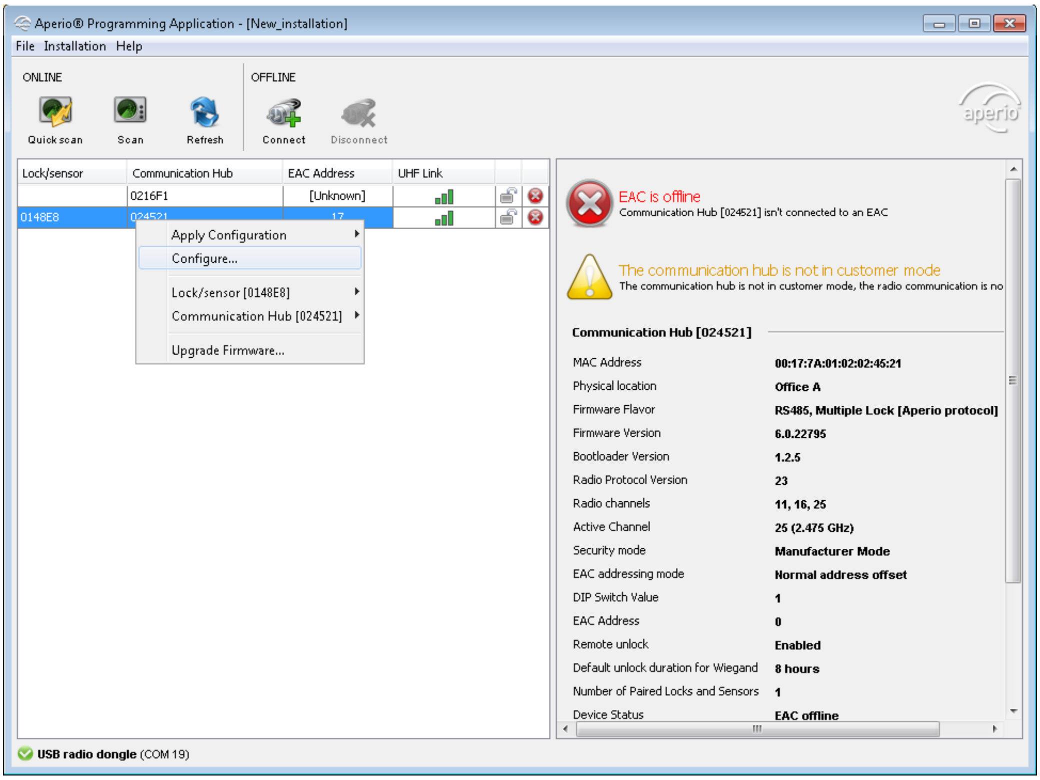


Pairing result
The result of the pairing request is presented below.

Communication hub paired successfully to:
0148ED

Configure function - Wizard

Open the configure function by right-clicking a communication hub or lock/sensor and selecting *Configure*.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
0148E8	024521	17	

EAC is offline
Communication Hub [024521] isn't connected to an EAC

The communication hub is not in customer mode
The communication hub is not in customer mode, the radio communication is no

Communication Hub [024521]

MAC Address	00:17:7A:01:02:02:45:21
Physical location	Office A
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.0.22795
Bootloader Version	1.2.5
Radio Protocol Version	23
Radio channels	11, 16, 25
Active Channel	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

USB radio dongle (COM 19)

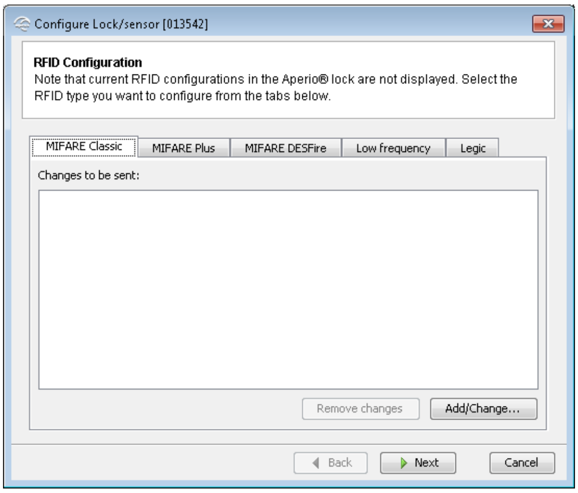
Depending on the hardware, different windows will appear in the wizard.

If more than one lock is paired to the communication hub the *Configure menu* is found on the *lock/sensor* and *communication hub* sub-menus respectively.

The following sections describe each window in the wizard.

RFID configuration (Lock/sensor)

A corresponding firmware for the given RFID type must be installed on the locks/sensors.
Click *Add/Change* to enter the settings for each credential type.



Configure Lock/sensor [013542]

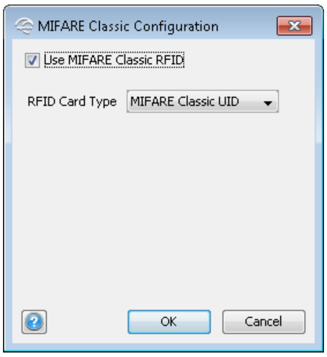
RFID Configuration

Note that current RFID configurations in the Aperio® lock are not displayed. Select the RFID type you want to configure from the tabs below.

Changes to be sent:

iCLASS RFID format is also supported by the programming application. However, no settings are necessary.

MIFARE Classic UID (Default)



MIFARE Classic Configuration

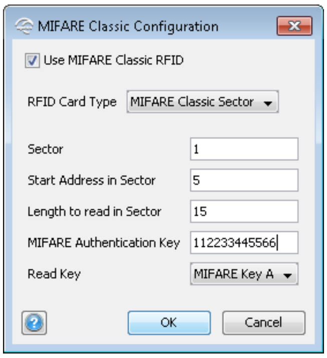
☑ Use MIFARE Classic RFID

RFID Card Type: MIFARE Classic UID

No settings are made to MIFARE Classic UID.
If you want to prevent MIFARE Classic from being read at all by the lock, uncheck *Use MIFARE Classic RFID*.

MIFARE Classic Sector

Select MIFARE Classic Sector in the RFID Card Type drop down list.



☑ Use MIFARE Classic RFID

RFID Card Type	MIFARE Classic Sector
Sector	1
Start Address in Sector	5
Length to read in Sector	15
MIFARE Authentication Key	112233445566
Read Key	MIFARE Key A

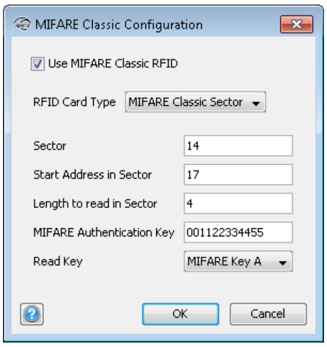
- **Start Address in Sector:** Parts of blocks within a sector can be used for credential data: 0 to 47 for 1K MIFARE Classic credentials. For 4K MIFARE Classic credential 0-47 (Start sector 0 to 31) and 0 – 239 (Start sector above 31).
- **Length to read in Sector:** Length of the credential data: 1 - 48 (Start sector above 31 cannot be used in the current release of the Programming Application).
- **MIFARE Authentication Key:** A 6 byte long hexadecimal key is required to read the credential data. For example: 112233445566.
- **Read Key:** Select the read key that the credential is configured to use for sector reading. The lock/sensor will give access only for this key.

ℹ If key B is selected as sector data read key, make sure that the access bits on the credential prevent reading of key B. If key B is readable on the credential, key B cannot be used to read the credential data.

Example:
To read the user data shown in the figure below, 17 10 19 80, and use the Authentication Key 001122334455 together with MIFARE Key A.

		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1		17	10	19	80												Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0	Manufacturer Data																Manufacturer Block

The configuration should look like this:



☑ Use MIFARE Classic RFID

RFID Card Type: MIFARE Classic Sector

Sector: 14

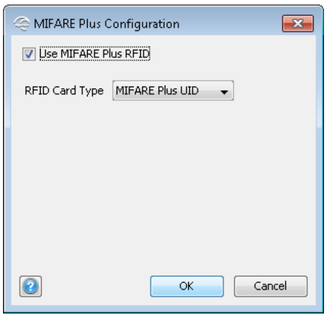
Start Address in Sector: 17

Length to read in Sector: 4

MIFARE Authentication Key: 001122334455

Read Key: MIFARE Key A

MIFARE Plus UID



MIFARE Plus Configuration

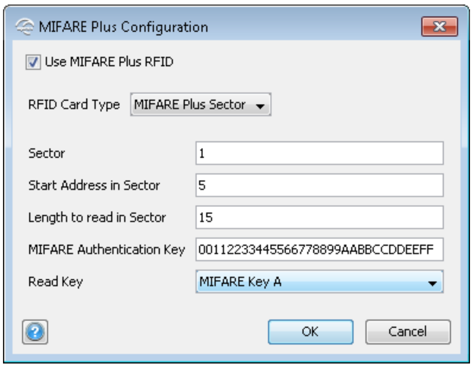
☑ Use MIFARE Plus RFID

RFID Card Type: MIFARE Plus UID

No settings are made to MIFARE Classic UID.
If you want to prevent MIFARE Plus UID from being read at all by the lock, uncheck *Use MIFARE Plus RFID*.

MIFARE Plus Sector

Select MIFARE Plus Sector in the RFID Card Type drop down list.



MIFARE Plus Configuration

☑ Use MIFARE Plus RFID

RFID Card Type: MIFARE Plus Sector

Sector: 1

Start Address in Sector: 5

Length to read in Sector: 15

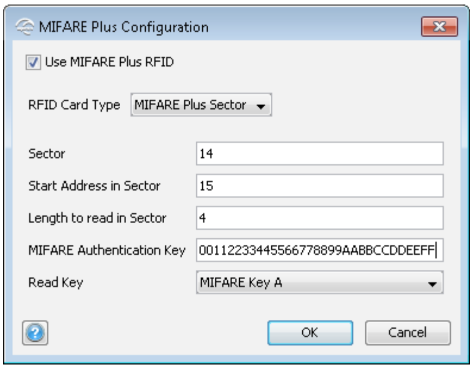
MIFARE Authentication Key: 00112233445566778899AABBCCDDEEFF

Read Key: MIFARE Key A

- **Start Address in Sector:** Parts of blocks within a sector can be used for credential data: 0 to 47 for 1K MIFARE Classic credentials. For 4K MIFARE Classic credentials 0-47 (Start sector 0 to 31) and 0 – 239 (Start sector above 31).
- **Length to read in Sector:** Length of the credential data: 1 - 48 (Start sector above 31 cannot be used in the current release of the Programming Application).
- **MIFARE Authentication Key:** A 16 byte long hexadecimal key is required to read the credential data. For example: 00112233445566778899AABBCCDDEEFF.
- **Read Key:** Select the read key that the credential is configured to use for sector reading. The lock will give access only for this key.

If key B is selected as sector data read key, make sure that the access bits on the credential prevent reading of key B. If key B is readable on the credential, key B cannot be used to read the credential data.

Example:
Since MIFARE Plus has the same memory organization as MIFARE Classic, we can use the same configuration. We will also use Key A but here the length of this key should be 16 byte, in this particular case: 00112233445566778899AABBCCDDEEFF.
The configuration should look like this:



MIFARE Plus Configuration

☑ Use MIFARE Plus RFID

RFID Card Type: MIFARE Plus Sector

Sector: 14

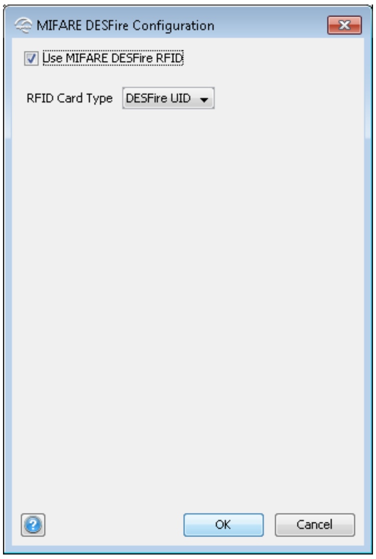
Start Address in Sector: 15

Length to read in Sector: 4

MIFARE Authentication Key: 00112233445566778899AABBCCDDEEFF

Read Key: MIFARE Key A

DESFire UID



MIFARE DESFire Configuration

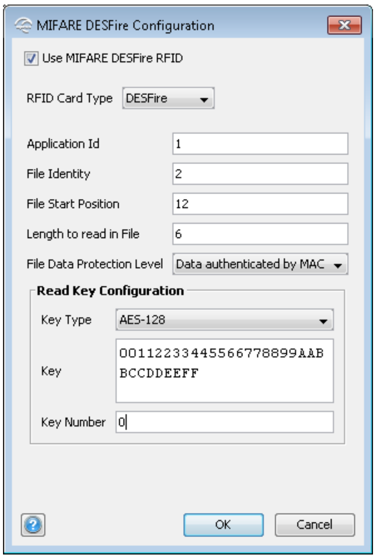
☑ Use MIFARE DESFire RFID

RFID Card Type: DESFire UID

No settings are made to DESFire UID.
If you want to prevent DESFire from being read at all by the lock, uncheck *Use DESFire RFID*.

DESFire

Select DESFire in the RFID Card Type drop down list.



MIFARE DESFire Configuration

☑ Use MIFARE DESFire RFID

RFID Card Type: DESFire

Application Id: 1

File Identity: 2

File Start Position: 12

Length to read in File: 6

File Data Protection Level: Data authenticated by MAC

Read Key Configuration

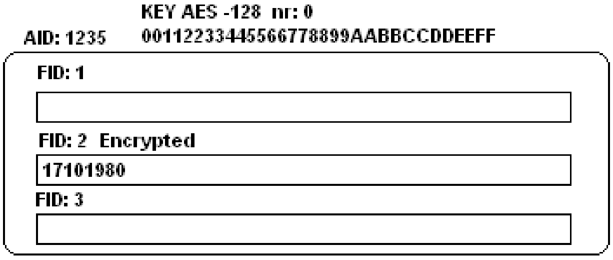
Key Type: AES-128

Key: 00112233445566778899AAB BCCDDEEFF

Key Number: 0

- **Application Id:** To configure the lock for file credential reading, you need to set first the Application Id of the application which contains the file. A credential can have up to 32 applications. Application Ids range from 0 to 16777215.
- **File Identity:** You need to type the File Id of the file you want to read. Every application can have up to 28 files. File Ids range is 1 to 255.
- **File Start Position:** You need to indicate the byte index where you want to start to read the file. If you type 0 it will start from the beginning of the file.
- **Length to read in File:** Type the length of the data you want to read. The length is specified in byte. Minimum length is 1 and the maximum length supported by the Aperio lock is 30 byte (this is the current limitation that will be removed in the future).
- **File Data Protection Level:** Select one of the three options (Plain, Data Authenticity by MAC, Full Encryption) depending on the data type of the file.
- **Key Type:** Select one of the four options (DES, 2K3DES, 3K3DES, AES-128) depending on the crypto used by your application's key. Type the key value in hexadecimal. DES, 2K3DES and AES-128 are 16 byte keys, 3K3DES is a 24 byte key.
- **Key Number:** Each application can store up to 14 keys. Key 0 is always the application's master key. Enter which key number from the application you want to use. Key numbers range from 0 to 13.

Example:



KEY AES -128 nr: 0

AID: 1235 00112233445566778899AABBCCDDEEFF

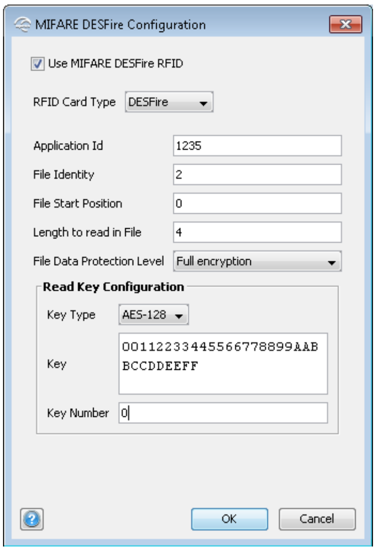
FID: 1

FID: 2 Encrypted

17101980

FID: 3

The configuration should look like this:



MIFARE DESFire Configuration

☑ Use MIFARE DESFire RFID

RFID Card Type: DESFire

Application Id: 1235

File Identity: 2

File Start Position: 0

Length to read in File: 4

File Data Protection Level: Full encryption

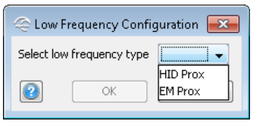
Read Key Configuration

Key Type: AES-128

Key: 00112233445566778899AAB
BCCDDEEFF

Key Number: 0

Low frequency



Low Frequency Configuration

Select low frequency type

In the list, select the low frequency credential type to use:

- HID Prox
- EM Prox

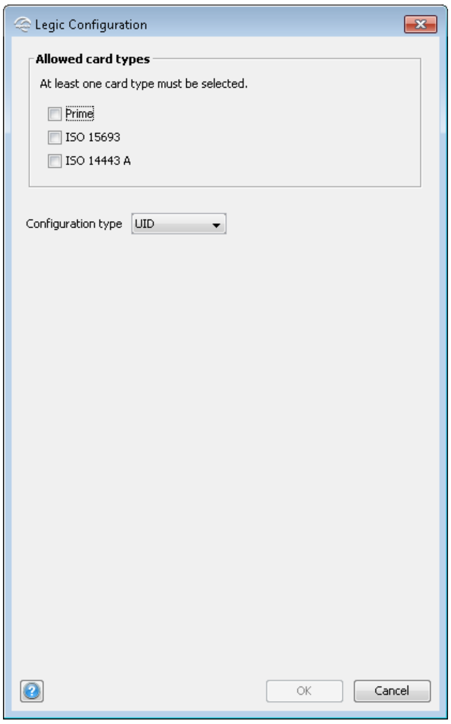
This credential type cannot be used together with any other credential types.

The following information is not applicable for the US market:
Before the lock/sensor has been configured with the Programming Application, the lock/ sensor will accept any Low Frequency credential technology.

Once the lock has read any credential technology 3 times the lock/sensor will only accept this technology. If the power is toggled the lock/sensor will return to the initial state of accepting any credential.

Once a specific credential technology has been configured via the Programming Application, this will be the only accepted type of credential. The lock will remain in this condition after the power has been toggled.

Legic UID


Legic Configuration

Allowed card types

At least one card type must be selected.

□ Prime
□ ISO 15693
□ ISO 14443 A

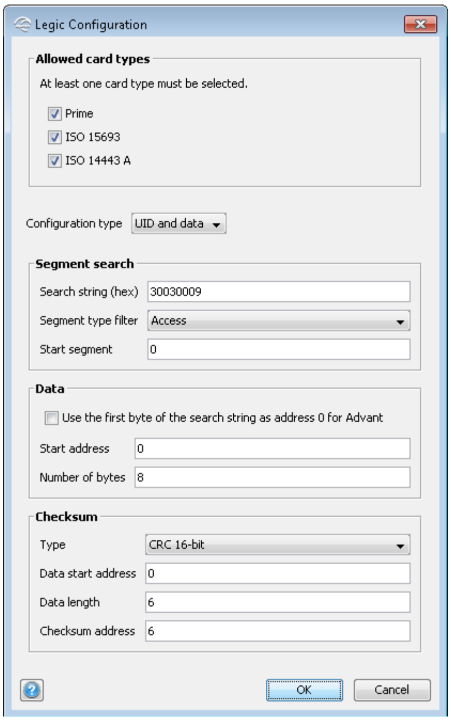
Configuration type: UID

In the list, select the card type to use:

- Prime
- ISO 15693 (Advant)
- ISO 14443 A (Advant)

No other settings are made to Legic UID.

Legic UID with data



Legic Configuration

Allowed card types

At least one card type must be selected.

☑ Prime
☑ ISO 15693
☑ ISO 14443 A

Configuration type: UID and data

Segment search

Search string (hex): 30030009
Segment type filter: Access
Start segment: 0

Data

□ Use the first byte of the search string as address 0 for Advant

Start address: 0
Number of bytes: 8

Checksum

Type: CRC 16-bit
Data start address: 0
Data length: 6
Checksum address: 6

In the list, select the card type to use:
- Prime
- ISO 15693 (Advant)
- ISO 14443 A (Advant)

Select UID with data in the drop down list.

Segment search:
- *Search string (hex):* Max 24 characters hexadecimal, even number of characters. For example: 30030009.
- *Segment type filter:* The type of segment, None, Access or Data.
- *Start segment:* Specifies the segment from which to start the search. It is useful in cases where more than one similar search string exists. Integer in the range of 0-255.

Data:
- *Use the first byte of the search string as address 0 for Advant:* Only for Advant card types, in order to change the data addressing of Advant. The first data byte will be the first search string/stamp byte.
- *Start address:* Specifies the start address of the data. Integer in the range of 0-255.
- *Number of byte:* Specifies the number of byte of data to be read. Integer in the range of 1-45.

Checksum:
- *Type:* "None" does not require any of the checksum related fields to be specified, but CRC 8-bit and 16-bit does.
- *Data start address:* Specifies the address where the data which checksum is to be calculated starts. Integer in the range of 0-255.

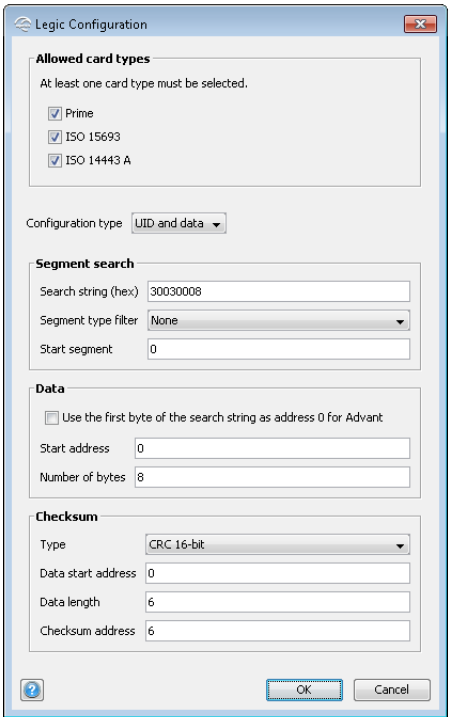
- *Data length:* Specifies the length of the data in number of byte to be read. Integer in the range of 0-255.
- *Checksum address:* Specifies the address where the checksum is located. Integer in the range of 0-255.

The credential data start address differs between Legic Prime and Legic Advant:

- For Legic Prime cards the first data byte starts with the first search string/stamp byte.
- For Legic Advant cards the first data byte starts with the first byte in the data area.

Example: Legic Advant Card

Segment 0:
Search String: 30 03 00 08
Segment type: Data
Data length: 8 byte
Checksum: CRC 16 byte 0-5
Checksum address: 6



Legic Configuration

Allowed card types

At least one card type must be selected.

☑ Prime
☑ ISO 15693
☑ ISO 14443 A

Configuration type: UID and data

Segment search

Search string (hex): 30030008
Segment type filter: None
Start segment: 0

Data

☐ Use the first byte of the search string as address 0 for Advant

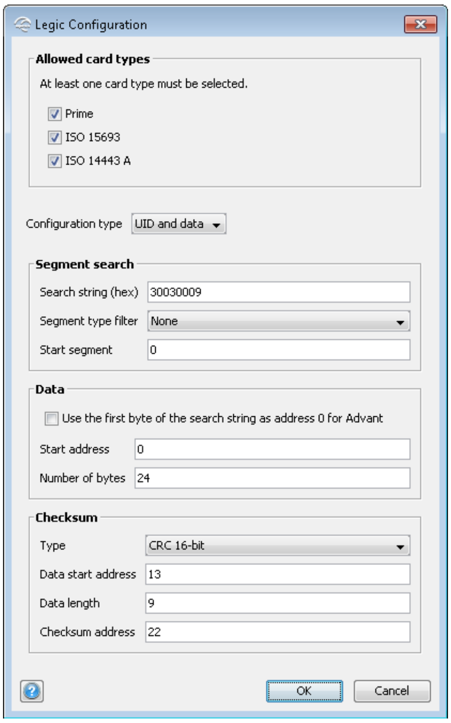
Start address: 0
Number of bytes: 8

Checksum

Type: CRC 16-bit
Data start address: 0
Data length: 6
Checksum address: 6

Segment 1:
Search String: 30 03 00 09
Segment type: Access
Data length: 24 byte
Checksum 1: CRC 16 byte 0-10
Checksum 1 address: 11

Checksum 2: CRC 16 byte 13-21
Checksum 2 address: 22


Legic Configuration

Allowed card types
At least one card type must be selected.
☑ Prime
☑ ISO 15693
☑ ISO 14443 A

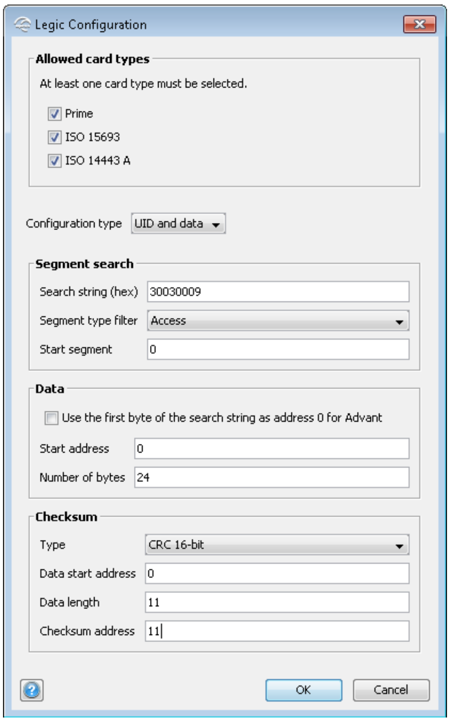
Configuration type: UID and data

Segment search
Search string (hex): 30030009
Segment type filter: None
Start segment: 0

Data
☐ Use the first byte of the search string as address 0 for Advant
Start address: 0
Number of bytes: 24

Checksum
Type: CRC 16-bit
Data start address: 13
Data length: 9
Checksum address: 22

or


Legic Configuration

Allowed card types
At least one card type must be selected.
☑ Prime
☑ ISO 15693
☑ ISO 14443 A

Configuration type: UID and data

Segment search
Search string (hex): 30030009
Segment type filter: Access
Start segment: 0

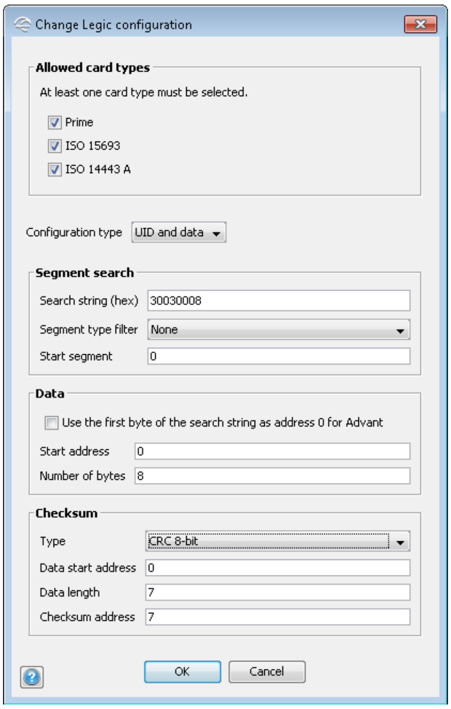
Data
☐ Use the first byte of the search string as address 0 for Advant
Start address: 0
Number of bytes: 24

Checksum
Type: CRC 16-bit
Data start address: 0
Data length: 11
Checksum address: 11

Only one checksum can be selected.

To include the search string in the first data byte, check the *Use the first byte of the search string as address 0 for Advant.*

Example: Legic Prime Card
Segment 0: (only segment)
Search String: 30 03 00 08
Segment type: Data
Data length: 8 byte
Checksum: CRC 8 byte 0-6
Checksum address: 7



Change Legic configuration

Allowed card types

At least one card type must be selected.

☑ Prime
☑ ISO 15693
☑ ISO 14443 A

Configuration type: UID and data

Segment search

Search string (hex): 30030008
Segment type filter: None
Start segment: 0

Data

□ Use the first byte of the search string as address 0 for Advant

Start address: 0
Number of bytes: 8

Checksum

Type: CRC 8-bit
Data start address: 0
Data length: 7
Checksum address: 7

RFID Search order for V2 SE and V3 locks (Lock)

When using V2 SE or V3 locks the search order of used RFID protocols can be specified. By changing the search order and/or disabling protocols not used, energy consumption and user waiting time can be reduced.

V2 locks does not support this setting.

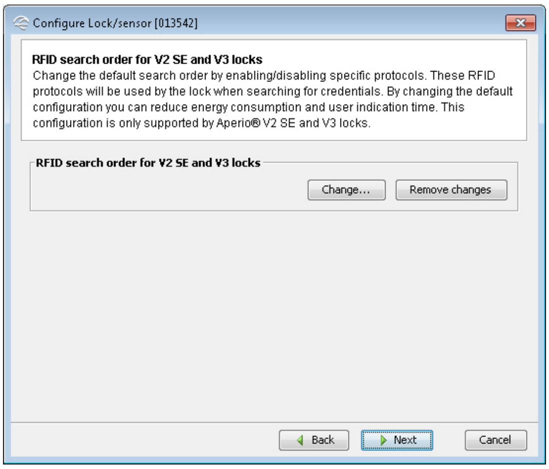
Important about RFID Search Configuration

If the RFID Search Configuration is done wrong, the lock may become inoperable. Be careful before changing these values.

Follow these guidelines:

- In installations where only one credential is used: Only enable corresponding RFID protocol.
- In installations with credentials using different RFID protocols: Change order so the most frequent RFID protocol is searched first.
- In installations where credential use may change over time: Do not change default configuration.

1) To enable and/or change search order of RFID protocols click *Change...*

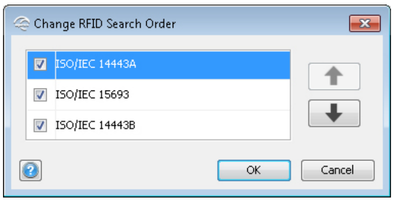


Configure Lock/sensor [013542]

RFID search order for V2 SE and V3 locks

Change the default search order by enabling/disabling specific protocols. These RFID protocols will be used by the lock when searching for credentials. By changing the default configuration you can reduce energy consumption and user indication time. This configuration is only supported by Aperio® V2 SE and V3 locks.

2) Select the protocols used and/or use the arrows to set the order the lock will perform a reading of a credential.



Change RFID Search Order

☑ ISO/IEC 14443A

☑ ISO/IEC 15693

☑ ISO/IEC 14443B

The mapping between RFID protocols and credentials are as follows:

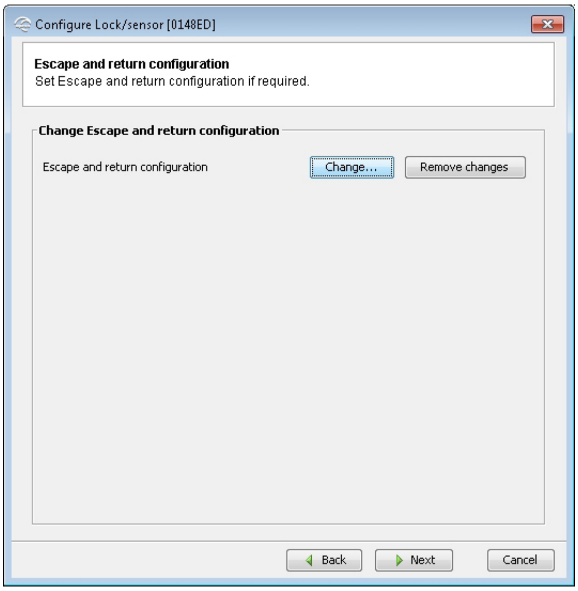
- ISO/IEC 14443A: MIFARE Classic, MIFARE DESFire, MIFARE Plus, iCLASS SEOS
- ISO/IEC 14443B: UID only
- ISO/IEC 15693: iCLASS

Escape and return configuration (Lock)

This function allows the lock to remain unlocked a certain time after the door have been opened from the inside.

This window is only visible if *Show advanced* settings is activated in the *Preferences* window, see section see section *"Preferences" on page* 9.

1) To set Escape and return configuration, click *Change...*



Configure Lock/sensor [0148ED]

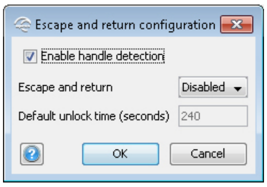
Escape and return configuration

Set Escape and return configuration if required.

Change Escape and return configuration

Escape and return configuration

2) Select desired settings:



Escape and return configuration

☑ Enable handle detection

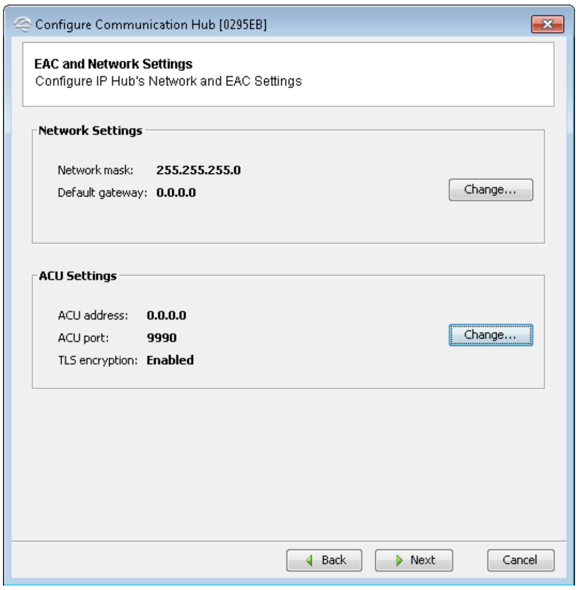
Escape and return: Disabled

Default unlock time (seconds): 240

- **Enable handle detection:** Enables the lock to register which handle was used to open the door, the inside or outside handle (lock side).
- **Escape and return:** Activate this function to either be Disabled or Enabled (in lock).
- **Default unlock time (seconds):** The time the lock is unlocked. Default is 240 seconds.

EAC and Network settings (AH40 communication hub)

This window only applies for AH40 communication hub (IP) in order to set the network and ACU settings for the installation site. This will allow maintenance such as firmware upgrade of the communication hub through the local network, instead of using the USB radio dongle.



Configure Communication Hub [0295EB]

EAC and Network Settings
Configure IP Hub's Network and EAC Settings

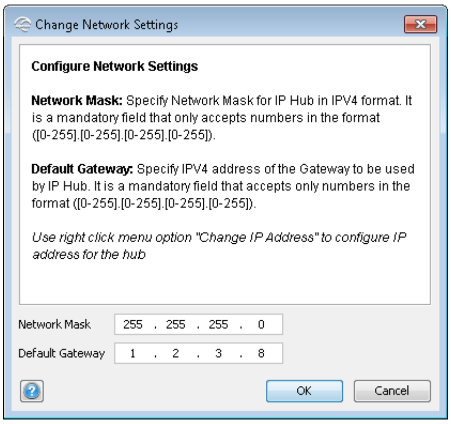
Network Settings

Network mask: **255.255.255.0**
Default gateway: **0.0.0.0**

ACU Settings

ACU address: **0.0.0.0**
ACU port: **9990**
TLS encryption: **Enabled**

Network settings



Change Network Settings

Configure Network Settings

Network Mask: Specify Network Mask for IP Hub in IPV4 format. It is a mandatory field that only accepts numbers in the format ([0-255].[0-255].[0-255].[0-255]).

Default Gateway: Specify IPV4 address of the Gateway to be used by IP Hub. It is a mandatory field that accepts only numbers in the format ([0-255].[0-255].[0-255].[0-255]).

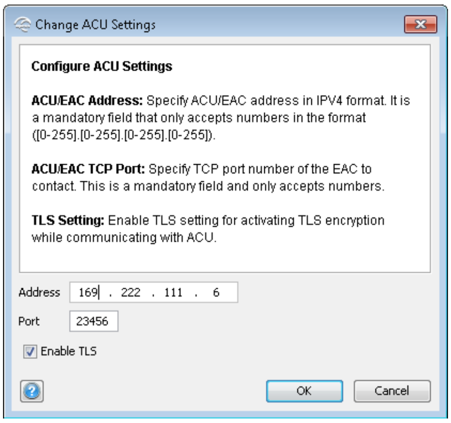
Use right click menu option "Change IP Address" to configure IP address for the hub

Network Mask 255 . 255 . 255 . 0
Default Gateway 1 . 2 . 3 . 8

For correct settings contact your network administrator:

- **Network Mask:** Network mask for the local network in IPV4 format, normally 255.255.255.0.
- **Default Gateway:** Default gateway for the local network in IPV4 format.

ACU settings



Configure ACU Settings

ACU/EAC Address: Specify ACU/EAC address in IPV4 format. It is a mandatory field that only accepts numbers in the format ([0-255].[0-255].[0-255].[0-255]).

ACU/EAC TCP Port: Specify TCP port number of the EAC to contact. This is a mandatory field and only accepts numbers.

TLS Setting: Enable TLS setting for activating TLS encryption while communicating with ACU.

Address 169 . 222 . 111 . 6

Port 23456

☑ Enable TLS

For correct settings contact your network/EAC administrator:

- **Address:** Network address for the EAC/ACU on the network. For example 192.168.0.155.
- **Port:** The TCP port of the EAC use for communication. Default value is 9990.
- **Enable TLS:** This setting provides secure communication between the EAC/ACU and the IP AH40 communication hub. The default value is enabled. Note that TLS must be enabled to allow customer mode to be set in the IP AH40 communication hub.

In order to establish a secure communication between the communication hub and the ACU, TLS is used. The sequence for connecting when in Manufacturer Mode is the following:

1) The communication hub makes a TCP connection to the ACU.

2) ACU and Hub will try to establish a TLS session. During TLS handshake, the ACU sends its certificate to the Hub.

3) Communication hub validates and stores the certificate.

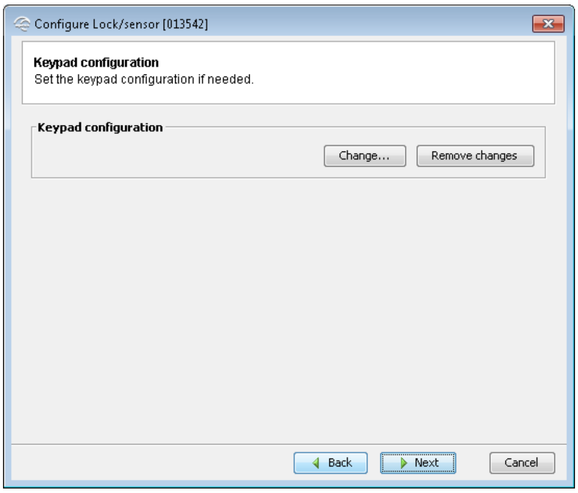
TLS specifies a number of possible cipher suites, but currently only TLS_RSA_WITH_AES_128_CBC_SHA is supported by the Hub. If a certificate using another cipher suite is used by the ACU, the Hub disconnects the TCP connection.

When in Customer Mode, the communication hub will only accept a TLS session where the previously stored certificate is presented. If any other certificate is presented, the communication hub will disconnect the TCP connection.

Advanced settings - Keypad configuration (Lock)

This window is only visible if *Show advanced settings* is activated in *Preferences*, see section *"Preferences" on page 9*.

1) Click *Change* to enter specific Keypad configuration.



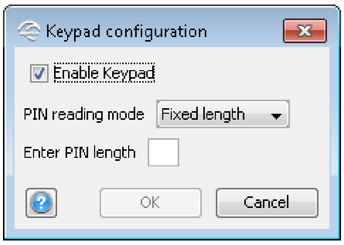
Configure Lock/sensor [013542]

Keypad configuration

Set the keypad configuration if needed.

Keypad configuration

2) Choose between two reading modes:



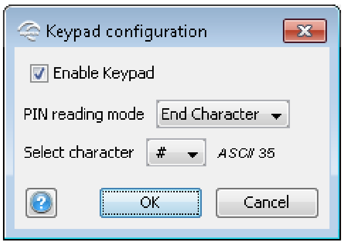
Keypad configuration

☑ Enable Keypad

PIN reading mode: Fixed length

Enter PIN length:

- **Fixed length:** PIN is set to use a fixed length.
- **Enter PIN length:** A value between 1 and 16, as specified by the EAC.



Keypad configuration

☑ Enable Keypad

PIN reading mode: End Character

Select character: # ASCII 35

- **End character:** PIN is sent to the EAC after an end character is pressed.
- **Select Character:** One of the non-numeric characters on the keypad can be used to submit the pin. For example: The user enters the PIN followed by a # on the keypad.

Override credential (Lock)

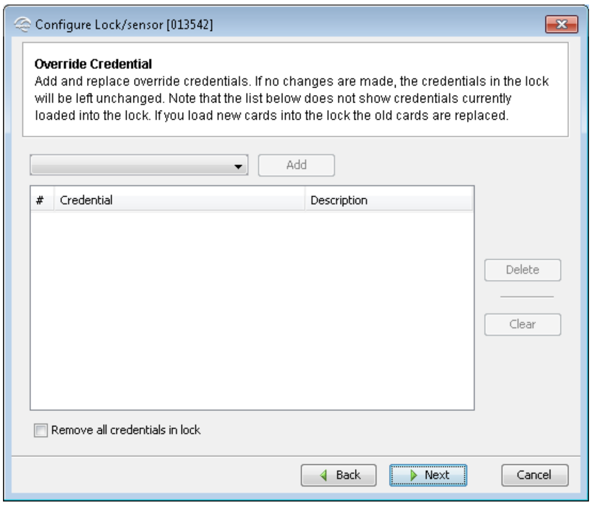
The override credentials are used to gain access to an area when the EAC is offline or when the lock has lost connection with the communication hub. Only the credentials from the override list will be granted access when the system is offline. You may add 10 override credentials to a lock.

Use of override credentials when using a Wiegand hub requires that DIP switch 1 is set to position ON.

When adding an override credentials in the lock all existing override credentials are removed from the lock.

Tip: You do not have to enter the override credential data manually for every lock to be configured. This can be saved using the *Save configuration* function as the last step of the configuration wizard. For remaining locks, use the *Apply configuration* function to apply the saved configuration.

1) To add an override credential, select the desired card type in the drop down list and click *Add*.



Configure Lock/sensor [013542]

Override Credential

Add and replace override credentials. If no changes are made, the credentials in the lock will be left unchanged. Note that the list below does not show credentials currently loaded into the lock. If you load new cards into the lock the old cards are replaced.

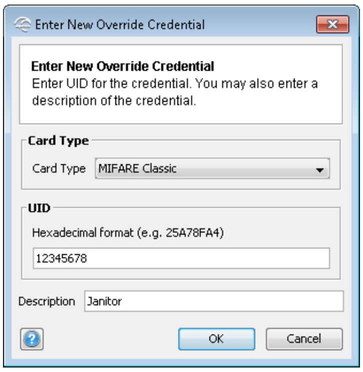
#	Credential	Description

□ Remove all credentials in lock

See the list below for a description of each credential.

If you check Remove all credentials in the lock, all existing override credentials in the lock will be deleted during the configuration process.

MIFARE UID



Enter New Override Credential
Enter UID for the credential. You may also enter a description of the credential.

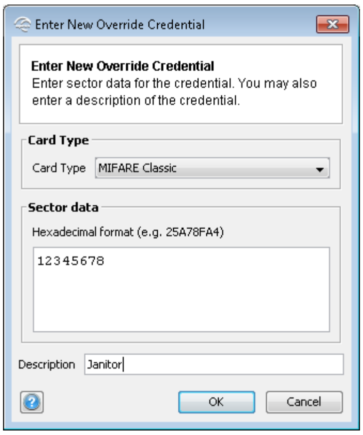
Card Type
Card Type: MIFARE Classic

UID
Hexadecimal format (e.g. 25A78FA4)
12345678

Description: Janitor

- **Card Type:** MIFARE Classic or MIFARE Plus.
- **UID:** Card number.
- **Description:** For example the credential owner.

MIFARE Sector



Enter New Override Credential
Enter sector data for the credential. You may also enter a description of the credential.

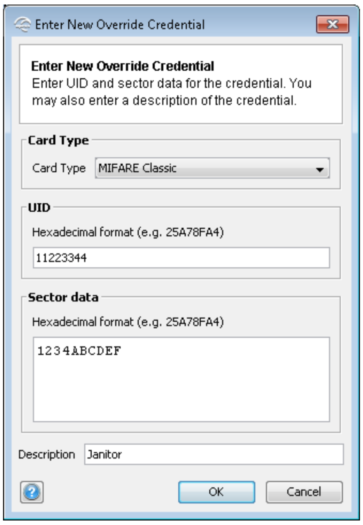
Card Type
Card Type: MIFARE Classic

Sector data
Hexadecimal format (e.g. 25A78FA4)
12345678

Description: Janitor

- **Card Type:** MIFARE Classic or MIFARE Plus.
- **Sector data:** Sector data stored on the credential. This value is normally stored in the EAC.
- **Description:** For example the credential owner.

MIFARE Sector and UID



Enter New Override Credential
Enter UID and sector data for the credential. You may also enter a description of the credential.

Card Type
Card Type: MIFARE Classic

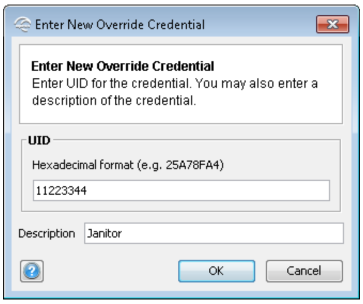
UID
Hexadecimal format (e.g. 25A78FA4)
11223344

Sector data
Hexadecimal format (e.g. 25A78FA4)
1234ABCDEF

Description: Janitor

- **Card Type:** MIFARE Classic or MIFARE Plus.
- **UID:** Card number.
- **Sector data:** Sector data stored on the credential. This value is normally stored in the EAC.
- **Description:** For example the credential owner.

ISO 14443B UID



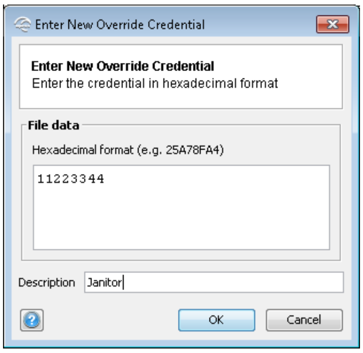
Enter New Override Credential
Enter UID for the credential. You may also enter a description of the credential.

UID
Hexadecimal format (e.g. 25A78FA4)
11223344

Description: Janitor

- **UID:** Card number.
- **Description:** For example the credential owner.

DESFire



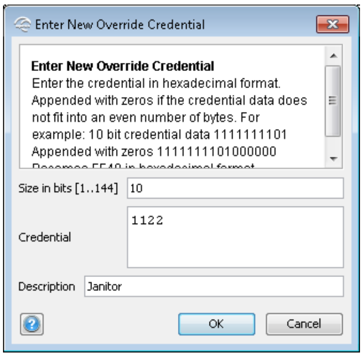
Enter New Override Credential
Enter the credential in hexadecimal format

File data
Hexadecimal format (e.g. 25A78FA4)
11223344

Description: Janitor

- **File data:** The file data stored on the credential.
- **Description:** For example the credential owner.

iCLASS

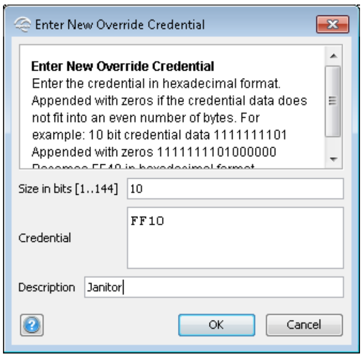


Enter New Override Credential
Enter the credential in hexadecimal format. Appended with zeros if the credential data does not fit into an even number of bytes. For example: 10 bit credential data 1111111101 Appended with zeros 1111111101000000

Size in bits [1..144]: 10
Credential: 1122
Description: Janitor

- **Size in bits [1...144]:** Number of bits used for credential data on the iCLASS credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

HID prox and EM prox

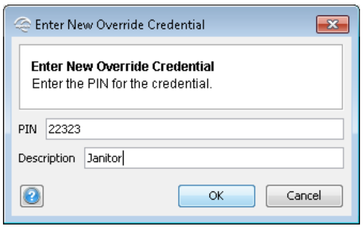


Enter New Override Credential
Enter the credential in hexadecimal format. Appended with zeros if the credential data does not fit into an even number of bytes. For example: 10 bit credential data 1111111101 Appended with zeros 1111111101000000

Size in bits [1..144]: 10
Credential: FF10
Description: Janitor

- **Size in bits [1...144]:** Number of bits used for credential data on the credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

PIN

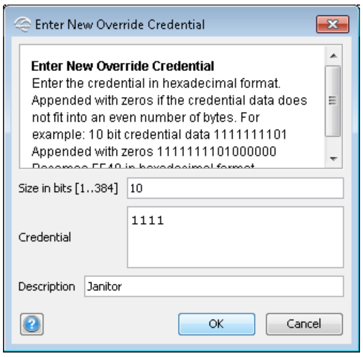


Enter New Override Credential
Enter the PIN for the credential.

PIN: 22323
Description: Janitor

- **PIN:** PIN code.
- **Description:** For example the PIN user.

Seos

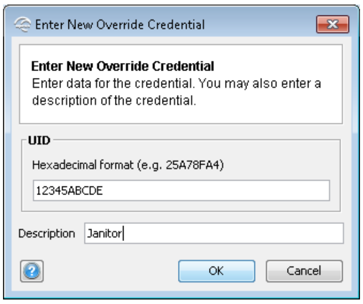


Enter New Override Credential
Enter the credential in hexadecimal format. Appended with zeros if the credential data does not fit into an even number of bytes. For example: 10 bit credential data 1111111101 Appended with zeros 1111111101000000

Size in bits [1..384]: 10
Credential: 1111
Description: Janitor

- **Size in bits [1...384]:** Number of bits used for credential data on the credential.
- **Credential:** Card credential appended with zeroes on the right side, and translated to hexadecimal format.
- **Description:** For example the credential owner.

Legic UID



Enter New Override Credential

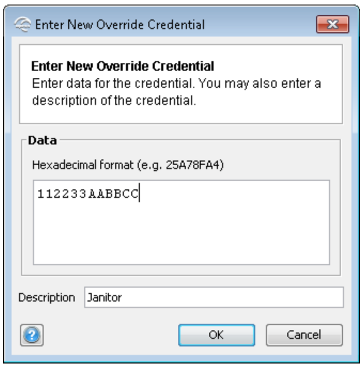
Enter New Override Credential
Enter data for the credential. You may also enter a description of the credential.

UID
Hexadecimal format (e.g. 25A78FA4)
12345ABCDE

Description: Janitor

- **UID:** Card number.
- **Description:** For example the credential owner.

Legic Data



Enter New Override Credential

Enter New Override Credential
Enter data for the credential. You may also enter a description of the credential.

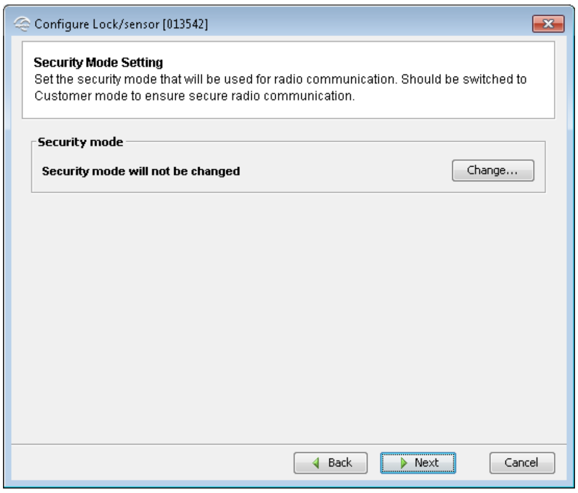
Data
Hexadecimal format (e.g. 25A78FA4)
112233AABBCC

Description: Janitor

- **Data:** Sector data stored on the credential.
- **Description:** For example the credential owner.

Security Mode Settings (Communication hub and Lock/sensor)

This setting will apply for both the communication hub and the lock if only one lock is paired.



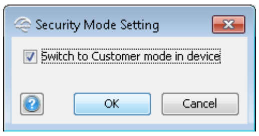
Configure Lock/sensor [013542]

Security Mode Setting
Set the security mode that will be used for radio communication. Should be switched to Customer mode to ensure secure radio communication.

Security mode
Security mode will not be changed

1) Click *Change* in the *Security Mode Setting* area if you want to change the security mode, or click *Next*.

2) To change to customer mode, check the checkbox and click *OK*.



Security Mode Setting

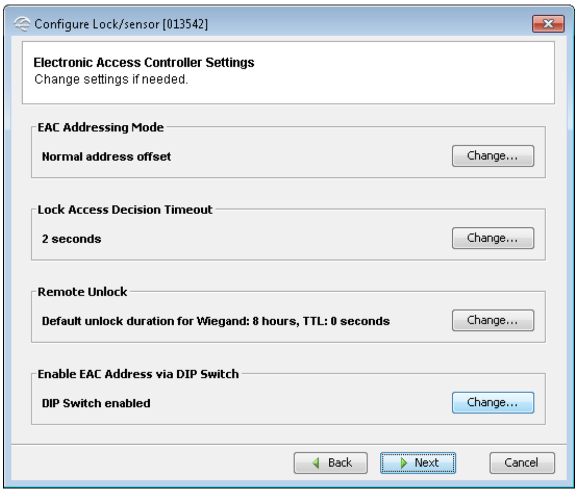
☑ Switch to Customer mode in device

The default mode is Manufacturer mode, but you should always change it to Customer mode. If you change to Manufacturer mode key the lock will no longer be using secure radio communication. Note that for IP AH40 communication hubs, TLS must also be enabled to allow customer mode to be set.

🔒	*Customer mode*	Lock is using secure radio communication with the customer encryption key.
🔓	*Manufacturer mode*	Lock is using insecure radio communication with the default encryption key.

Electronic Access Controller settings (Communication hub)

The following options apply for both RS-485 and Wiegand unless specified. Click *Change...* for each option, to enter the settings.



Configure Lock/sensor [013542]

Electronic Access Controller Settings
Change settings if needed.

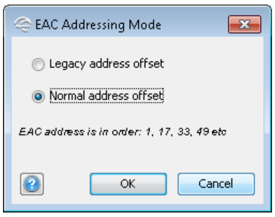
EAC Addressing Mode: **Normal address offset**

Lock Access Decision Timeout: **2 seconds**

Remote Unlock: **Default unlock duration for Wiegand: 8 hours, TTL: 0 seconds**

Enable EAC Address via DIP Switch: **DIP Switch enabled**

EAC Addressing Mode (RS-485 only)



EAC Addressing Mode

○ Legacy address offset

● Normal address offset

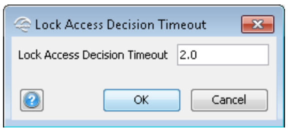
EAC address is in order: 1, 17, 33, 49 etc

The default EAC addressing mode is Normal address offset, which means that the communication hub assigns the EAC address to the paired locks according to the addressing table, see the Aperio Online Mechanical Installation manual. This setting is used when the EAC can handle addresses without limit.

Legacy address offset is used when the EAC has a low limit for handling addresses, for example 32 or 64. The following example shows the addresses assigned to the locks on a communication hub with address 1:

- **Normal address offset:** 1,17,33, 49 and so on.
    - **Legacy address offset:** 1, 2, 3, 4, 5, 6, 7, 8 (communication hub 1), (9-16 for communication hub 2, 17-24 for communication hub 3 and so on).

Lock Access Decision Timeout

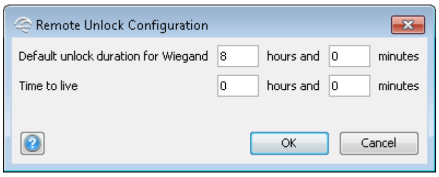


Lock Access Decision Timeout

Lock Access Decision Timeout: 2.0

This value sets the time (in seconds) the lock will wait for an access decision from the EAC.

Remote unlock



Remote Unlock Configuration

Default unlock duration for Wiegand: 8 hours and 0 minutes

Time to live: 0 hours and 0 minutes

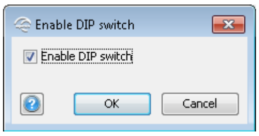
This function enables the Remote unlock functionality in the communication hub.

- **Default unlock duration for Wiegand:** Enter the time the lock will be unlocked after the lock performs a status report. To deactivate *Remote Unlock*, set the time to 0. This setting only applies for Wiegand communication hubs (Unlock duration is set in the EAC for RS-485 communication hubs).
- **Time to live:** The time for how long the *Remote unlock* command will be present in the communication hub. The maximum value is 17 hours and 59 minutes. (This setting must always be longer than the Status Report interval set in the lock.) This setting only applies for RS-485 communication hubs.

RS-485 communication hubs (firmware version 2.6.5 or later): Remote unlock is by default enabled in the communication hub.

RS-485 communication hubs (firmware version earlier than 2.6.5): Activate Remote unlock by clicking *OK*, since this is disabled in the firmware by default.

Enable EAC Address via DIP Switch (RS-485 only)



Enable DIP switch

☑ Enable DIP switch

Checking the *Enable DIP Switch* checkbox will restore the EAC addressing to what is configured with the DIP switches on the communication hub.

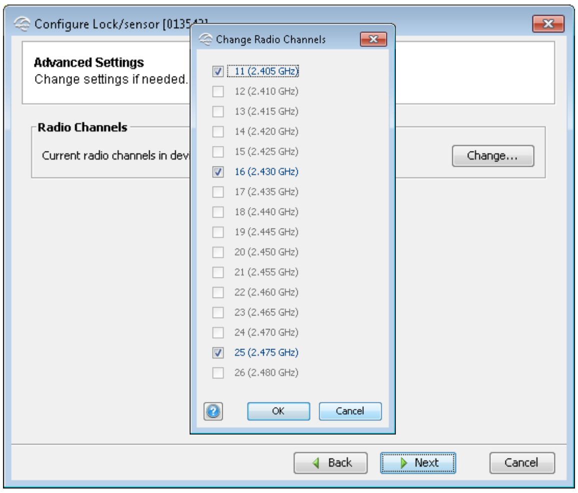
To disable the DIP switch the EAC address must digitally be set as well. To do this use the *Change the EAC address* function on the right-click menu for the communication hub.

Advanced setting - Radio channel settings (Communication hub or Lock/sensor)

Always change the radio channel on the lock before changing on the communication hub.

This function is also available on the right-click menu in the *installation view*.

1) Click *Change...* to set the radio channel the communication.



Configure Lock/sensor [01354?]

Advanced Settings
Change settings if needed.

Radio Channels
Current radio channels in dev

Change Radio Channels

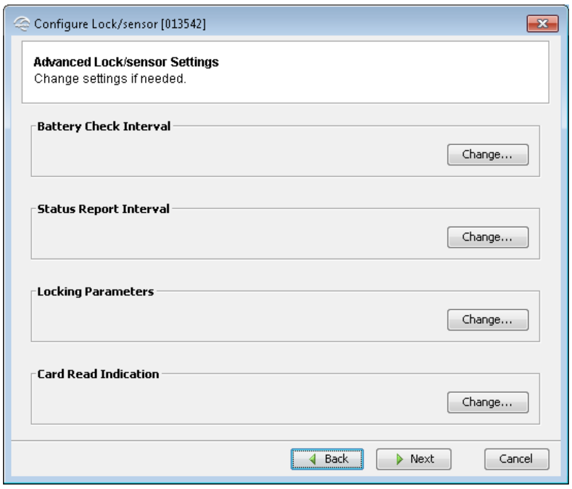
☑ 11 (2.405 GHz)
□ 12 (2.410 GHz)
□ 13 (2.415 GHz)
□ 14 (2.420 GHz)
□ 15 (2.425 GHz)
☑ 16 (2.430 GHz)
□ 17 (2.435 GHz)
□ 18 (2.440 GHz)
□ 19 (2.445 GHz)
□ 20 (2.450 GHz)
□ 21 (2.455 GHz)
□ 22 (2.460 GHz)
□ 23 (2.465 GHz)
□ 24 (2.470 GHz)
☑ 25 (2.475 GHz)
□ 26 (2.480 GHz)

2) Deselect one or several of the used channels to make a new selection of channels.

For the US market channel 26 is disabled.

Advanced Lock/sensor Settings - Online

These settings allow configuration of *Battery Power Alarm Interva*l, *Status Report Interval*, *Locking Parameters*, *Card Read Indication*, including *Sensor Events* and *Polling Interval found on the following page*.



Configure Lock/sensor [013542]

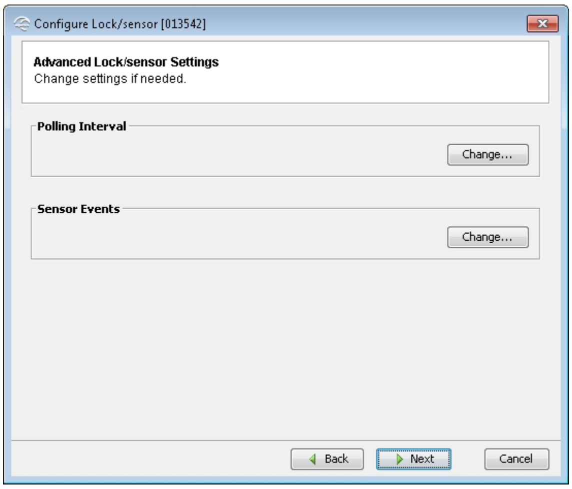
Advanced Lock/sensor Settings
Change settings if needed.

Battery Check Interval

Status Report Interval

Locking Parameters

Card Read Indication



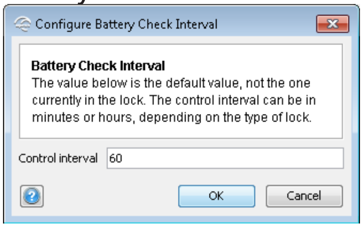
Configure Lock/sensor [013542]

Advanced Lock/sensor Settings
Change settings if needed.

Polling Interval

Sensor Events

Battery Check Interval



Battery Check Interval

The value below is the default value, not the one currently in the lock. The control interval can be in minutes or hours, depending on the type of lock.

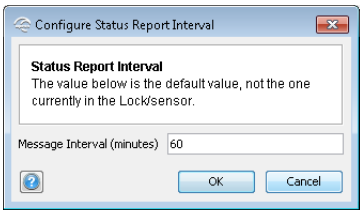
Control interval: 60

The battery power check is sent from the lock to the EAC system and is used to indicate when it is time to replace the battery. It may be necessary to adjust the time interval for this check depending on the type of battery used and the surrounding temperature, e.g. in cold surroundings the battery runs out faster. Default value is 60 (minutes).

For products with battery measurement on the secure side (P100/I100 currently), the interval you set translates into hours, i.e. 6 minutes = 6 hours on those products.

Status Report Interval

This setting applies to both lock/sensor and communication hub.



Status Report Interval

The value below is the default value, not the one currently in the Lock/sensor.

Message Interval (minutes): 60

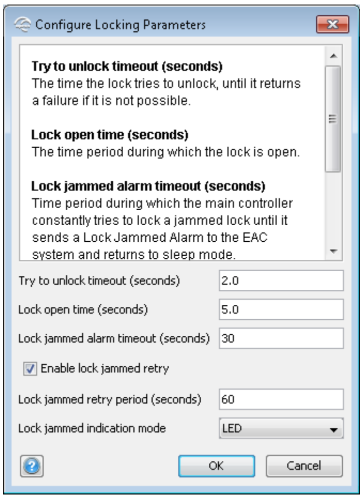
The interval setting is normally set to 60 minutes. If *Remote Unlock* functionality is used, this parameter should be set to a shorter interval such somewhere in between 5 and 15 minutes or depending on the time the remote unlock command is present in the communication hub.

Lowering the status interval time for any reason will have an adverse effect on the battery life of the product.

As the status report interval is used by the communication hub to detect if the lock has gone offline, any changes to this interval must be done on both lock and communication hub. If one lock is paired with the communication hub this is done automatically.

If more than one lock is paired with the communication hub (AH30 and AH40) the status report interval must be set through the communication hub right-click menu to a value equal or higher then the longest interval of the locks paired.

Locking Parameters



Try to unlock timeout (seconds)
The time the lock tries to unlock, until it returns a failure if it is not possible.

Lock open time (seconds)
The time period during which the lock is open.

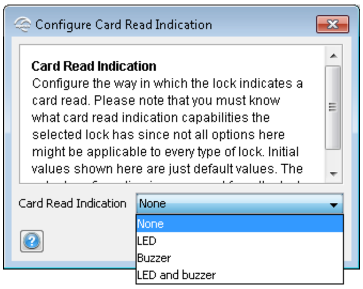
Lock jammed alarm timeout (seconds)
Time period during which the main controller constantly tries to lock a jammed lock until it sends a Lock Jammed Alarm to the EAC system and returns to sleep mode.

Try to unlock timeout (seconds) 2.0
Lock open time (seconds) 5.0
Lock jammed alarm timeout (seconds) 30
☑ Enable lock jammed retry
Lock jammed retry period (seconds) 60
Lock jammed indication mode LED

This dialog allows you to configure timing for different operations in the lock:

- **Try to unlock timeout (seconds):** How long the lock tries to unlock before it returns a failure.
- **Lock open time (seconds):** How long the lock will be open in seconds (default = 5 seconds).
- **Lock jammed alarm timeout (seconds):** How long time the system tries to lock the lock before it sends an alarm to the EAC and goes back to idle state (default = 30 seconds).
- **Enable lock jammed retry:** This enables a periodic retry to lock the lock according the settings under "Lock jammed retry period (seconds).
- **Lock jammed retry period (seconds):** How long the lock will wait before it retries to lock, in seconds (default = 60 seconds).
- **Lock jammed indication mode:** The way in which the lock indicates that it has been jammed. LED, Buzzer and LED and buzzer are the different indication modes.

Card Read Indication

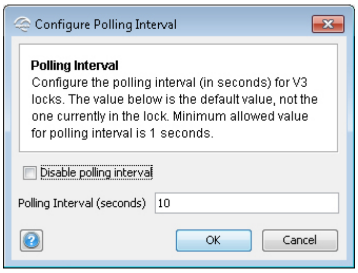


Card Read Indication
Configure the way in which the lock indicates a card read. Please note that you must know what card read indication capabilities the selected lock has since not all options here might be applicable to every type of lock. Initial values shown here are just default values. The

Card Read Indication None

Different locks can have a different mechanism for audio-visual indication of successful credential reading. Here it is possible to disable credential read indication or to set it to LED. Some Aperio locks have support for other mechanisms such as buzzers.

Polling interval (V3 locks)



Polling Interval
Configure the polling interval (in seconds) for V3 locks. The value below is the default value, not the one currently in the lock. Minimum allowed value for polling interval is 1 seconds.

□ Disable polling interval

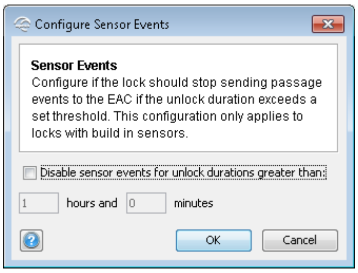
Polling Interval (seconds) 10

This setting only applies for V3 locks. The polling interval decides how often the lock wakes up and connects to the communication hub to check for information from the EAC (Unlike a status report, see section *"Status Report Interval" on page 42*, where the lock status information is also sent to the EAC.).

Polling also allows the Programming application to connect to the lock without the need of activating the radio with a credential (if the polling interval is set to less than 15 seconds). Default polling interval in the lock is 10 seconds.

To change this, enter a new polling interval here. Polling can be deactivated in lock by checking Disable polling interval.

Sensor Events



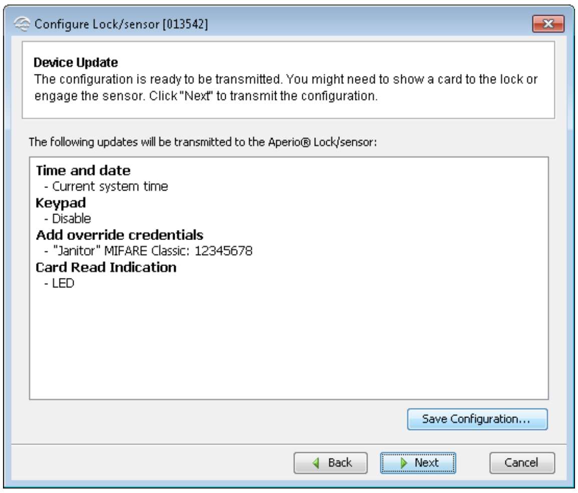
Sensor Events
Configure if the lock should stop sending passage events to the EAC if the unlock duration exceeds a set threshold. This configuration only applies to locks with build in sensors.

□ Disable sensor events for unlock durations greater than:

1 hours and 0 minutes

This setting applies for locks with built in sensor. By activating this function, the lock sensor will stop sending passage events to the EAC for unlock durations longer than you set here. This setting will save battery life in high traffic doors.

Device update page – Saving Configuration



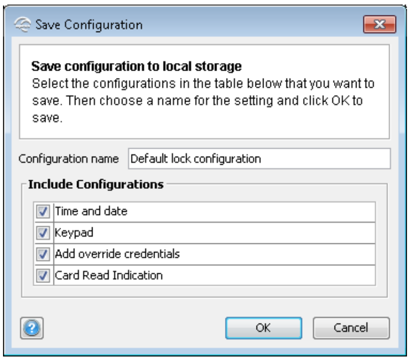
Device Update
The configuration is ready to be transmitted. You might need to show a card to the lock or engage the sensor. Click "Next" to transmit the configuration.

The following updates will be transmitted to the Aperio® Lock/sensor:

Time and date
- Current system time
Keypad
- Disable
Add override credentials
- "Janitor" MIFARE Classic: 12345678
Card Read Indication
- LED

The Device Update dialog shows a summary of the configuration tasks that will be downloaded to communication hub/lock/sensor. The configuration may be used later to configure other devices with the same information, by clicking *Save configuration*:

1) The Save Configuration dialog box shows a summary of the configuration tasks that have been collected during the different steps in the Configuration Wizard. Exclude configuration tasks by clicking the check boxes.



Save configuration to local storage
Select the configurations in the table below that you want to save. Then choose a name for the setting and click OK to save.

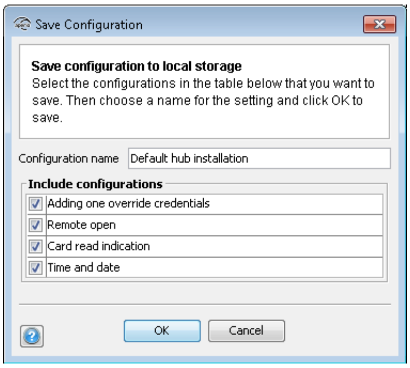
Configuration name: Default lock configuration

Include Configurations
☑ Time and date
☑ Keypad
☑ Add override credentials
☑ Card Read Indication

2) Recommended tasks to save could be:
- RFID configuration
- Change security mode
- Override credential
- Device time update
- And optionally some advanced features like Battery Alarm, Status configuration and Locking parameters.

If you choose to save a configuration, keep in mind that some configuration settings should not be saved. Only save settings that are general for all locks in your installation. **Tip:** Create a set of configurations for the most common settings in your system.

3) Enter a unique and suitable name for this configuration in the Configuration name field. Choose this name carefully, to make it clear what settings are changed in the lock/sensor or communication hub. You could, for instance, name it according to the different configuration tasks or, if applicable, use a name that reflects the specific door type.



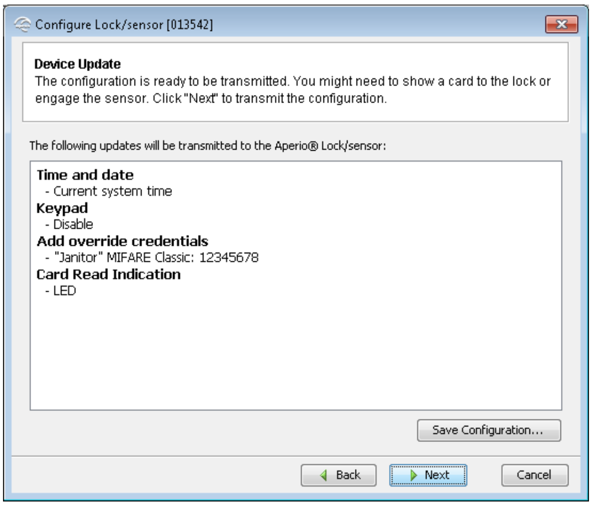
Save configuration to local storage
Select the configurations in the table below that you want to save. Then choose a name for the setting and click OK to save.

Configuration name: Default hub installation

Include configurations
- ☑ Adding one override credentials
- ☑ Remote open
- ☑ Card read indication
- ☑ Time and date

4) Click *OK*.

Result: The configuration is saved in the local storage and the *Save configuration* window is closed. Clicking *Cancel* on the *Device Update* page does not affect the locally stored configuration.



Device Update
The configuration is ready to be transmitted. You might need to show a card to the lock or engage the sensor. Click "Next" to transmit the configuration.

The following updates will be transmitted to the Aperio® Lock/sensor:

Time and date
- Current system time

Keypad
- Disable

Add override credentials
- "Janitor" MIFARE Classic: 12345678

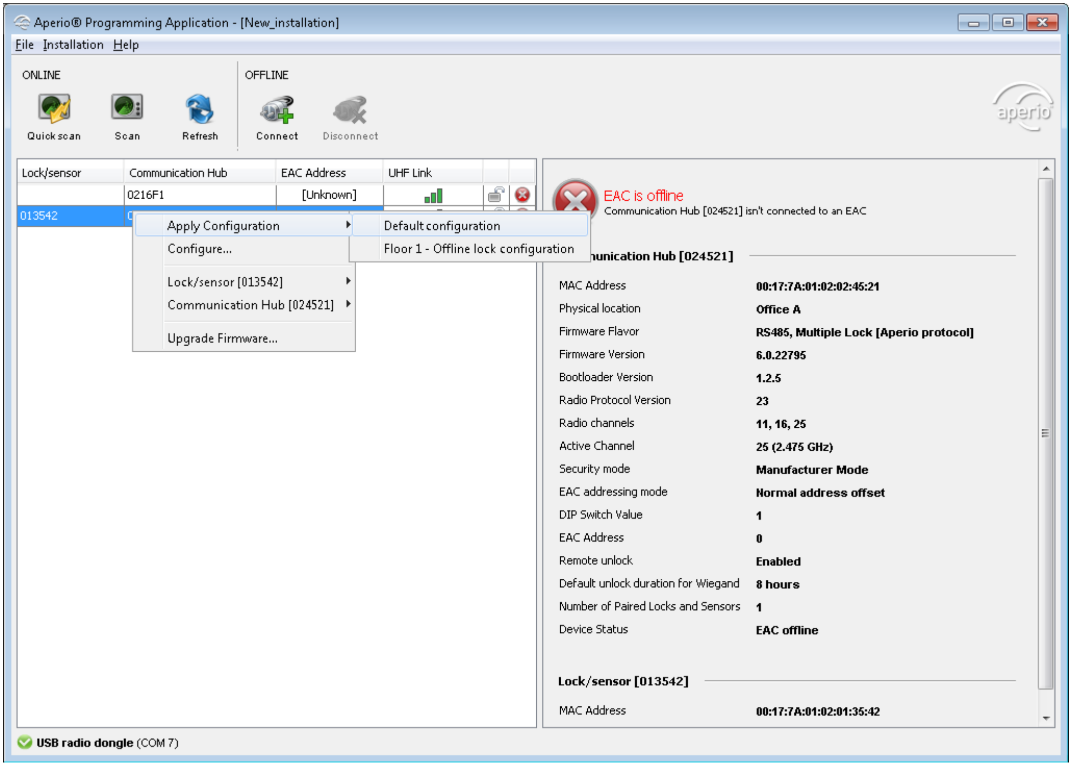
Card Read Indication
- LED

Applying a stored configuration to a communication hub/lock/sensor

If you saved a configuration in the configuration wizard, you can apply it to numerous locks/sensors. This function is available on both the Lock/sensor menu and the communication hub menu and will only download settings that apply for the hardware selected.

Follow these steps to download a saved configuration to a lock/sensor:

1) In the *Installation view*, right-click the desired communication hub&lock/sensor and select *Apply configuration* and an earlier stored configuration.



EAC is offline
Communication Hub [024521] isn't connected to an EAC

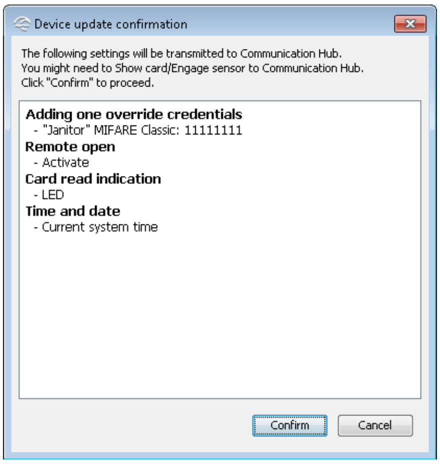
unication Hub [024521]

MAC Address	00:17:7A:01:02:02:45:21
Physical location	Office A
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.0.22795
Bootloader Version	1.2.5
Radio Protocol Version	23
Radio channels	11, 16, 25
Active Channel	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

MAC Address	00:17:7A:01:02:01:35:42

2) Click *Confirm* to download the selected configuration to the unit.



The following settings will be transmitted to Communication Hub.
You might need to Show card/Engage sensor to Communication Hub.
Click "Confirm" to proceed.

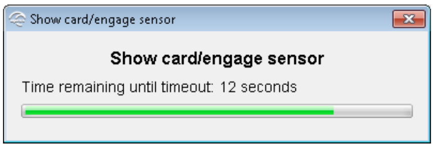
Adding one override credentials
- "Janitor" MIFARE Classic: 11111111

Remote open
- Activate

Card read indication
- LED

Time and date
- Current system time

3) Hold the credential at the lock, or engage the magnet for the sensor, to download the configuration. (This will not be required when downloading configuration to a communication hub.)

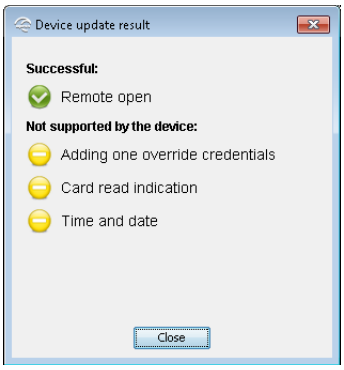


Show card/engage sensor

Show card/engage sensor

Time remaining until timeout: 12 seconds

4) After download the result is shown. The settings that could not be transferred to the specific hardware are ignored. Click *Close* to finish.



Device update result

Successful:

✓ Remote open

Not supported by the device:

⊖ Adding one override credentials

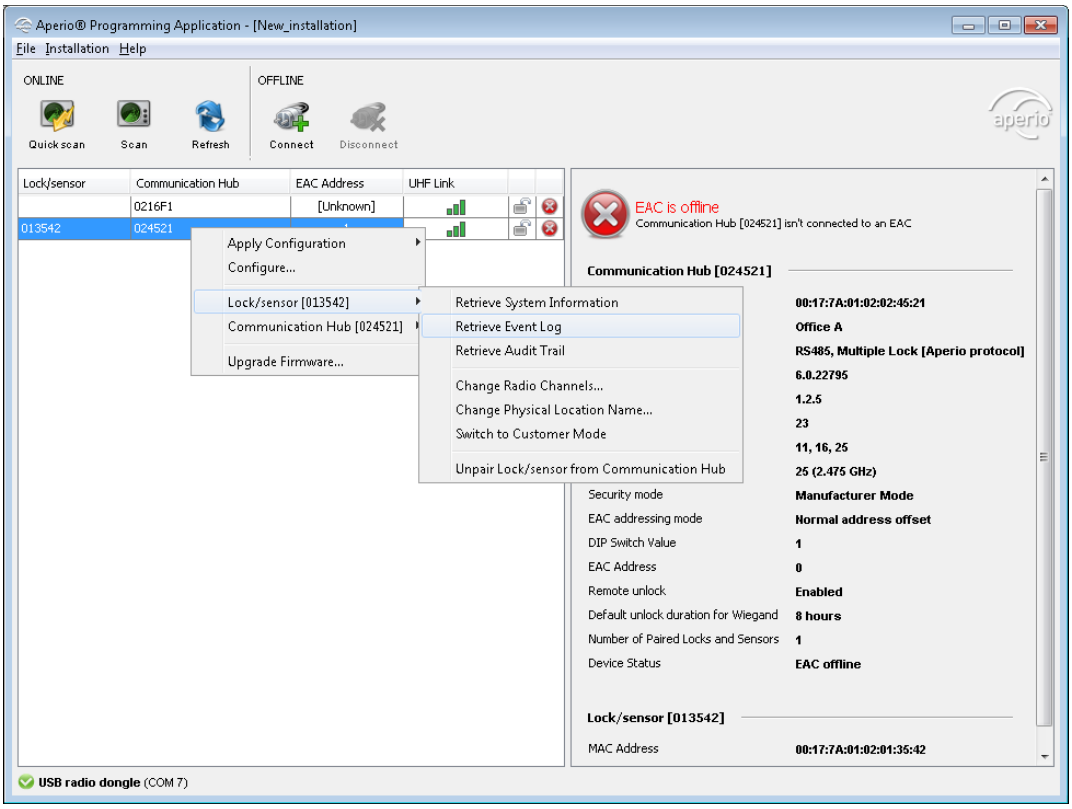
⊖ Card read indication

⊖ Time and date

5) Repeat all the steps from the beginning of this section for every lock/sensor you want to configure with a saved configuration. Click *Close* to finish.

Retrieve system information

This function is available for both communication hub and lock/sensors.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521		

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

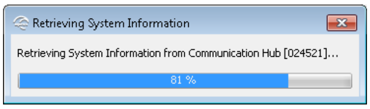
	00:17:7A:01:02:02:45:21
	Office A
	RS485, Multiple Lock [Aperio protocol]
	6.0.22795
	1.2.5
	23
	11, 16, 25
	25 (2.475 GHz)
Security mode	**Manufacturer Mode**
EAC addressing mode	**Normal address offset**
DIP Switch Value	**1**
EAC Address	**0**
Remote unlock	**Enabled**
Default unlock duration for Wiegand	**8 hours**
Number of Paired Locks and Sensors	**1**
Device Status	**EAC offline**

Lock/sensor [013542]

MAC Address	**00:17:7A:01:02:01:35:42**

USB radio dongle (COM 7)

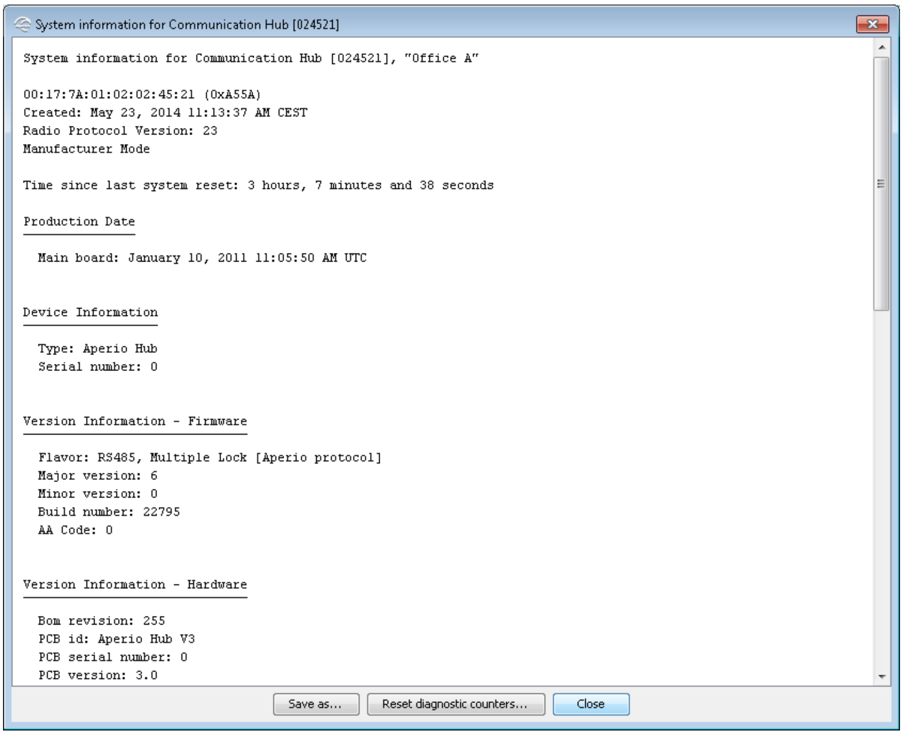
1) Right-click and select *Lock/sensor* or *Communication Hub – Retrieve system information* to access the unit.



Retrieving System Information from Communication Hub [024521]...

Result: The Programming Application connects to the unit.

2) Click *Save as...* to save the system information to a local storage, Click *Reset diagnostic counters...* to reset the diagnostic counters in the device or click *Close* to exit.



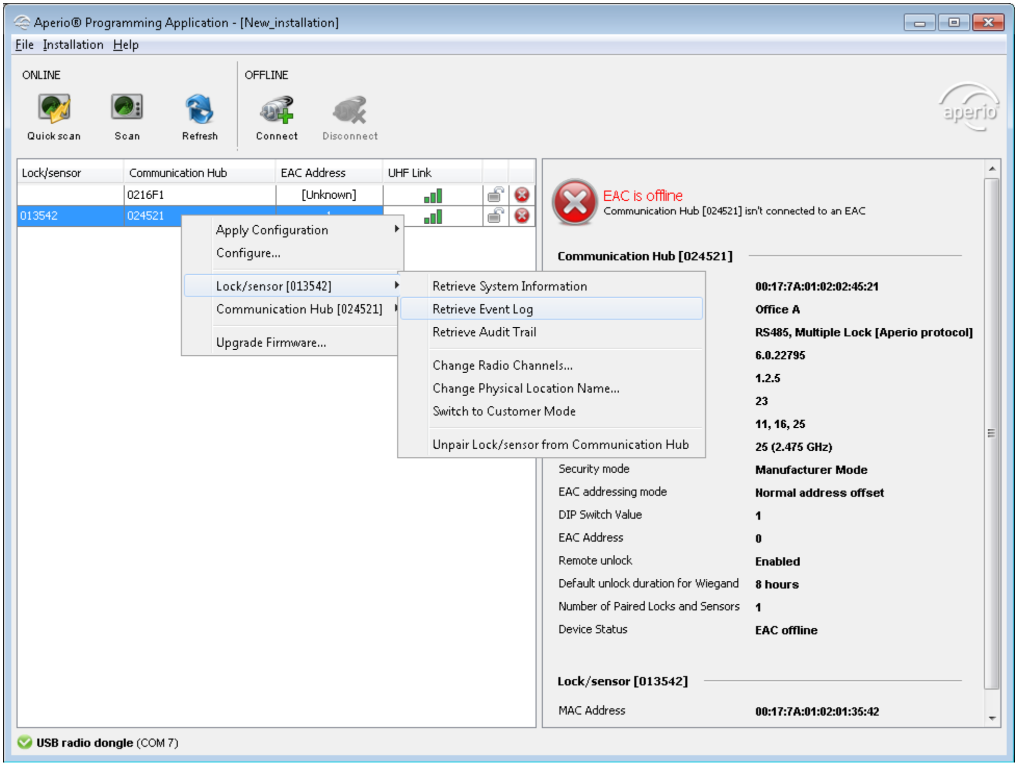
System information for Communication Hub [024521]
Save as...
Reset diagnostic counters...
Close

```
System information for Communication Hub [024521], "Office A"

00:17:7A:01:02:02:45:21 (0xA55A)
Created: May 23, 2014 11:13:37 AM CEST
Radio Protocol Version: 23
Manufacturer Mode

Time since last system reset: 3 hours, 7 minutes and 38 seconds

Production Date

  Main board: January 10, 2011 11:05:50 AM UTC


Device Information

  Type: Aperio Hub
  Serial number: 0


Version Information - Firmware

  Flavor: RS485, Multiple Lock [Aperio protocol]
  Major version: 6
  Minor version: 0
  Build number: 22795
  AA Code: 0


Version Information - Hardware

  Bom revision: 255
  PCB id: Aperio Hub V3
  PCB serial number: 0
  PCB version: 3.0
```

Retrieve Event Log

This function displays the event log for a particular lock or IP AH40 communication hub (not available for sensor), where you can find all system events performed on the lock. In the example below the event log is retrieved from a lock.

1) Right-click and select *Lock/sensor – Retrieve Event Log...*



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521		

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

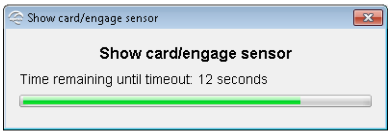
	00:17:7A:01:02:02:45:21
	Office A
	RS485, Multiple Lock [Aperio protocol]
	6.0.22795
	1.2.5
	23
	11, 16, 25
	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

MAC Address	00:17:7A:01:02:01:35:42

USB radio dongle (COM 7)

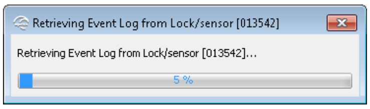
2) Hold the credential at the lock.



Show card/engage sensor

Time remaining until timeout: 12 seconds

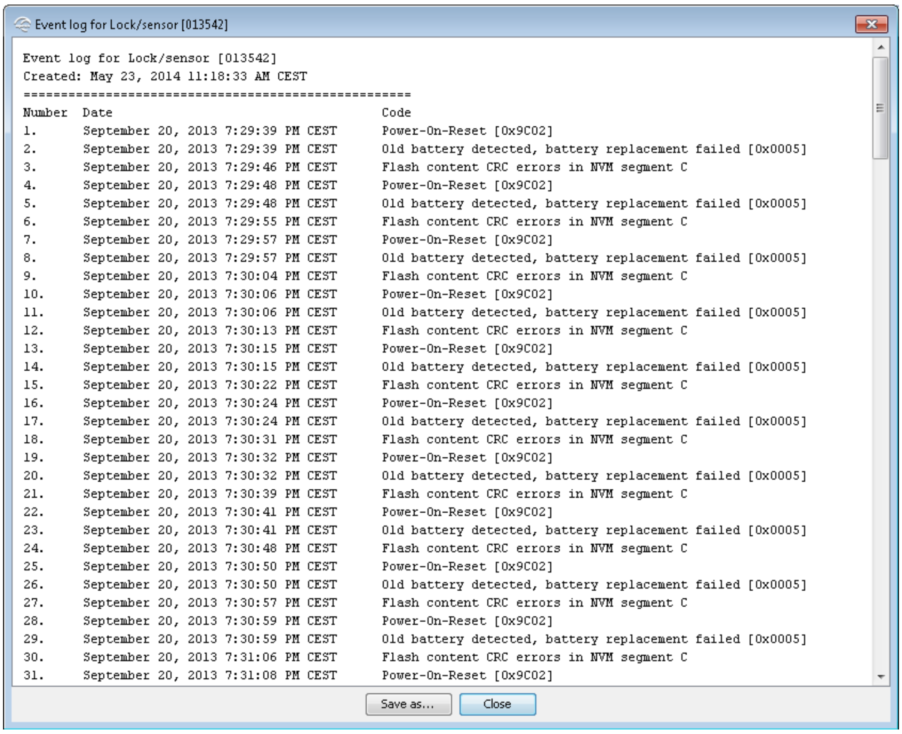
Result: Successful reading initiates the download of the event log.



Retrieving Event Log from Lock/sensor [013542]...

5 %

3) In the event log window, click *Save As...* to save the information to a *.txt-file or click *Close* to exit without saving.



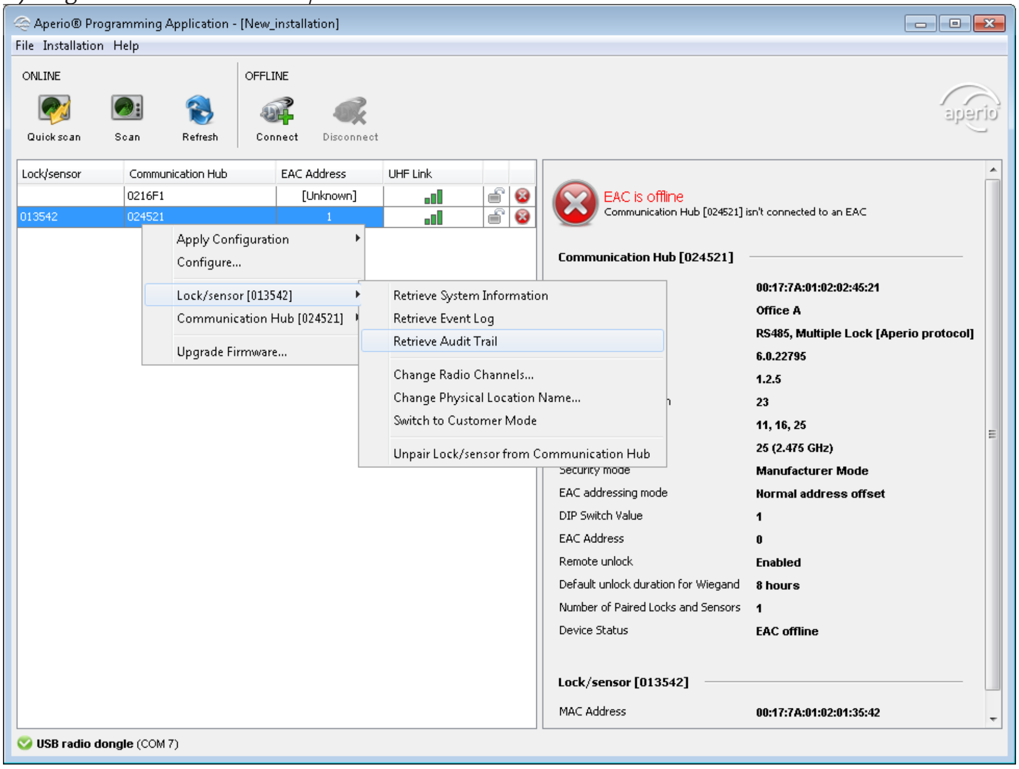
```
Event log for Lock/sensor [013542]
Created: May 23, 2014 11:18:33 AM CEST
====================================================
Number  Date                                    Code
1.      September 20, 2013 7:29:39 PM CEST      Power-On-Reset [0x9C02]
2.      September 20, 2013 7:29:39 PM CEST      Old battery detected, battery replacement failed [0x0005]
3.      September 20, 2013 7:29:46 PM CEST      Flash content CRC errors in NVM segment C
4.      September 20, 2013 7:29:48 PM CEST      Power-On-Reset [0x9C02]
5.      September 20, 2013 7:29:48 PM CEST      Old battery detected, battery replacement failed [0x0005]
6.      September 20, 2013 7:29:55 PM CEST      Flash content CRC errors in NVM segment C
7.      September 20, 2013 7:29:57 PM CEST      Power-On-Reset [0x9C02]
8.      September 20, 2013 7:29:57 PM CEST      Old battery detected, battery replacement failed [0x0005]
9.      September 20, 2013 7:30:04 PM CEST      Flash content CRC errors in NVM segment C
10.     September 20, 2013 7:30:06 PM CEST      Power-On-Reset [0x9C02]
11.     September 20, 2013 7:30:06 PM CEST      Old battery detected, battery replacement failed [0x0005]
12.     September 20, 2013 7:30:13 PM CEST      Flash content CRC errors in NVM segment C
13.     September 20, 2013 7:30:15 PM CEST      Power-On-Reset [0x9C02]
14.     September 20, 2013 7:30:15 PM CEST      Old battery detected, battery replacement failed [0x0005]
15.     September 20, 2013 7:30:22 PM CEST      Flash content CRC errors in NVM segment C
16.     September 20, 2013 7:30:24 PM CEST      Power-On-Reset [0x9C02]
17.     September 20, 2013 7:30:24 PM CEST      Old battery detected, battery replacement failed [0x0005]
18.     September 20, 2013 7:30:31 PM CEST      Flash content CRC errors in NVM segment C
19.     September 20, 2013 7:30:32 PM CEST      Power-On-Reset [0x9C02]
20.     September 20, 2013 7:30:32 PM CEST      Old battery detected, battery replacement failed [0x0005]
21.     September 20, 2013 7:30:39 PM CEST      Flash content CRC errors in NVM segment C
22.     September 20, 2013 7:30:41 PM CEST      Power-On-Reset [0x9C02]
23.     September 20, 2013 7:30:41 PM CEST      Old battery detected, battery replacement failed [0x0005]
24.     September 20, 2013 7:30:48 PM CEST      Flash content CRC errors in NVM segment C
25.     September 20, 2013 7:30:50 PM CEST      Power-On-Reset [0x9C02]
26.     September 20, 2013 7:30:50 PM CEST      Old battery detected, battery replacement failed [0x0005]
27.     September 20, 2013 7:30:57 PM CEST      Flash content CRC errors in NVM segment C
28.     September 20, 2013 7:30:59 PM CEST      Power-On-Reset [0x9C02]
29.     September 20, 2013 7:30:59 PM CEST      Old battery detected, battery replacement failed [0x0005]
30.     September 20, 2013 7:31:06 PM CEST      Flash content CRC errors in NVM segment C
31.     September 20, 2013 7:31:08 PM CEST      Power-On-Reset [0x9C02]
```

The window contains information of system events including consecutive number, date, and what type of system event that was performed. (If the number of events exceeds 200 older events are overwritten.)

Retrieve Audit Trail

This function displays a complete list of all access attempts for a particular lock (not available for sensor).

1) Right-click and select *Lock/sensor – Retrieve Audit Trail*.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521	1	

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

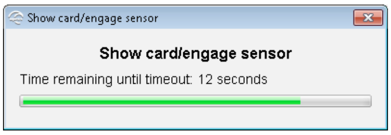
	00:17:7A:01:02:02:45:21
	Office A
	RS485, Multiple Lock [Aperio protocol]
	6.0.22795
	1.2.5
	23
	11, 16, 25
	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

MAC Address	00:17:7A:01:02:01:35:42

USB radio dongle (COM 7)

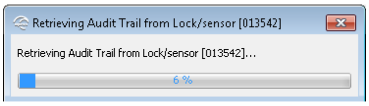
2) Hold the credential at the lock.



Show card/engage sensor

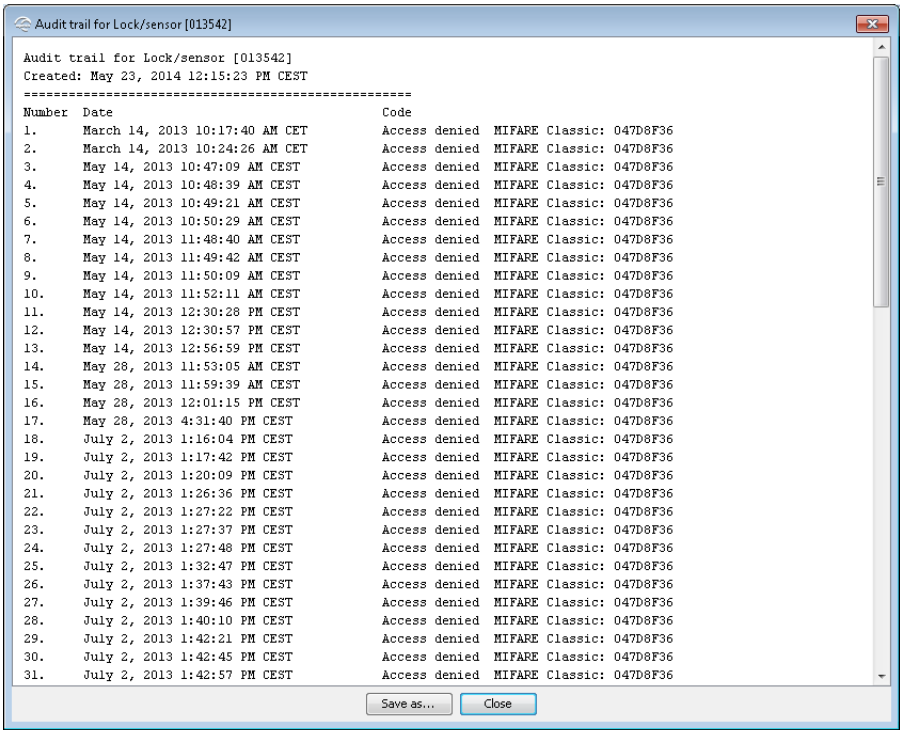
Time remaining until timeout: 12 seconds

Result: Successful reading initiates the download of the audit trail.



Retrieving Audit Trail from Lock/sensor [013542]...

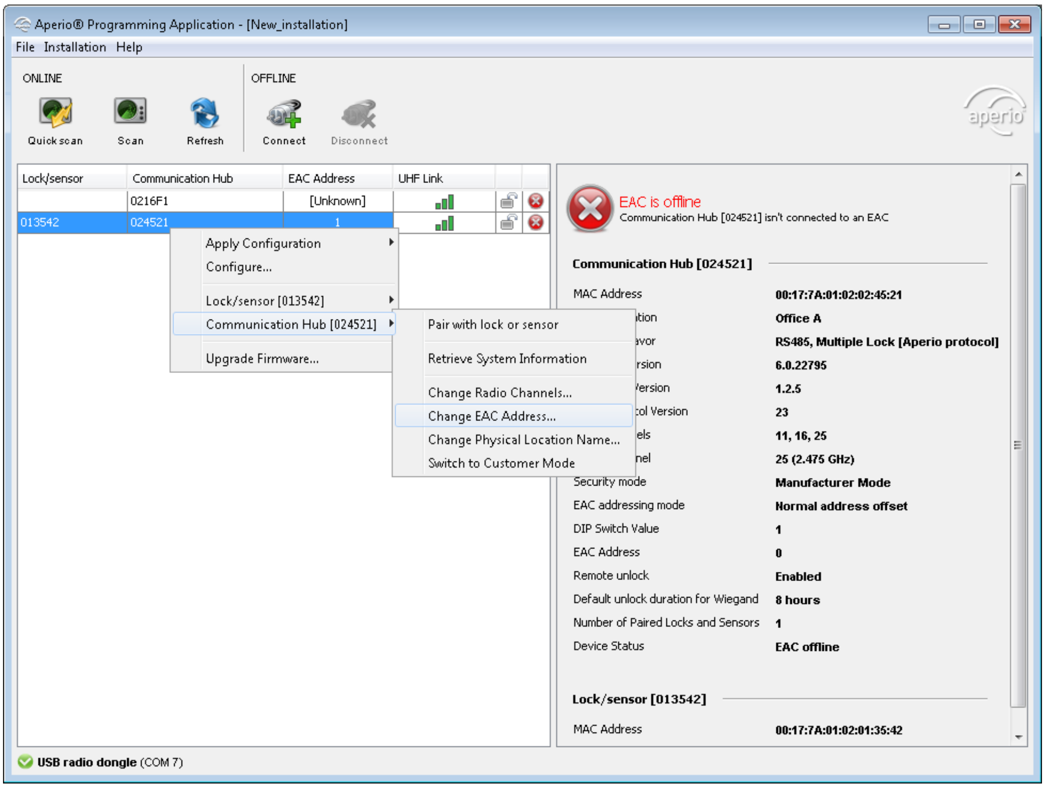
3) In the audit trail window, click *Save As...* to save the information to a *.txt-file or click *Close* to exit without saving.



```
Audit trail for Lock/sensor [013542]
Created: May 23, 2014 12:15:23 PM CEST
====================================================
Number  Date                                    Code
1.      March 14, 2013 10:17:40 AM CET          Access denied  MIFARE Classic: 047D8F36
2.      March 14, 2013 10:24:26 AM CET          Access denied  MIFARE Classic: 047D8F36
3.      May 14, 2013 10:47:09 AM CEST           Access denied  MIFARE Classic: 047D8F36
4.      May 14, 2013 10:48:39 AM CEST           Access denied  MIFARE Classic: 047D8F36
5.      May 14, 2013 10:49:21 AM CEST           Access denied  MIFARE Classic: 047D8F36
6.      May 14, 2013 10:50:29 AM CEST           Access denied  MIFARE Classic: 047D8F36
7.      May 14, 2013 11:48:40 AM CEST           Access denied  MIFARE Classic: 047D8F36
8.      May 14, 2013 11:49:42 AM CEST           Access denied  MIFARE Classic: 047D8F36
9.      May 14, 2013 11:50:09 AM CEST           Access denied  MIFARE Classic: 047D8F36
10.     May 14, 2013 11:52:11 AM CEST           Access denied  MIFARE Classic: 047D8F36
11.     May 14, 2013 12:30:28 PM CEST           Access denied  MIFARE Classic: 047D8F36
12.     May 14, 2013 12:30:57 PM CEST           Access denied  MIFARE Classic: 047D8F36
13.     May 14, 2013 12:56:59 PM CEST           Access denied  MIFARE Classic: 047D8F36
14.     May 28, 2013 11:53:05 AM CEST           Access denied  MIFARE Classic: 047D8F36
15.     May 28, 2013 11:59:39 AM CEST           Access denied  MIFARE Classic: 047D8F36
16.     May 28, 2013 12:01:15 PM CEST           Access denied  MIFARE Classic: 047D8F36
17.     May 28, 2013 4:31:40 PM CEST            Access denied  MIFARE Classic: 047D8F36
18.     July 2, 2013 1:16:04 PM CEST            Access denied  MIFARE Classic: 047D8F36
19.     July 2, 2013 1:17:42 PM CEST            Access denied  MIFARE Classic: 047D8F36
20.     July 2, 2013 1:20:09 PM CEST            Access denied  MIFARE Classic: 047D8F36
21.     July 2, 2013 1:26:36 PM CEST            Access denied  MIFARE Classic: 047D8F36
22.     July 2, 2013 1:27:22 PM CEST            Access denied  MIFARE Classic: 047D8F36
23.     July 2, 2013 1:27:37 PM CEST            Access denied  MIFARE Classic: 047D8F36
24.     July 2, 2013 1:27:48 PM CEST            Access denied  MIFARE Classic: 047D8F36
25.     July 2, 2013 1:32:47 PM CEST            Access denied  MIFARE Classic: 047D8F36
26.     July 2, 2013 1:37:43 PM CEST            Access denied  MIFARE Classic: 047D8F36
27.     July 2, 2013 1:39:46 PM CEST            Access denied  MIFARE Classic: 047D8F36
28.     July 2, 2013 1:40:10 PM CEST            Access denied  MIFARE Classic: 047D8F36
29.     July 2, 2013 1:42:21 PM CEST            Access denied  MIFARE Classic: 047D8F36
30.     July 2, 2013 1:42:45 PM CEST            Access denied  MIFARE Classic: 047D8F36
31.     July 2, 2013 1:42:57 PM CEST            Access denied  MIFARE Classic: 047D8F36
```

The window contains information on the total number of access attempts including consecutive number, date, access decision and what type of credential that was used at each attempt.

Change EAC address



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521	1	

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

MAC Address	00:17:7A:01:02:02:45:21
tion	Office A
avor	RS485, Multiple Lock [Aperio protocol]
rsion	6.0.22795
ersion	1.2.5
col Version	23
els	11, 16, 25
nel	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

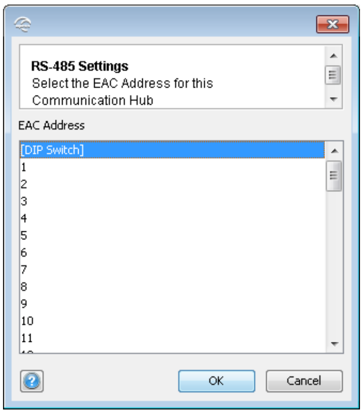
MAC Address	00:17:7A:01:02:01:35:42

USB radio dongle (COM 7)

It is recommended to use the DIP Switch for setting the EAC address of communication hubs. However, if needed the *Change EAC address* function allows you to digitally assign an EAC address in the range of 1-63 (1-15 for communication hubs with several locks/sensors paired and 1-63 for communication hubs with one lock/sensor paired).

If the Programming Application is used to set RS 485 addresses, it will override the address set by the DIP switch on the communication hub.

1) Right-click and select *Communication hub– Change EAC Address*.



RS-485 Settings
Select the EAC Address for this Communication Hub

EAC Address

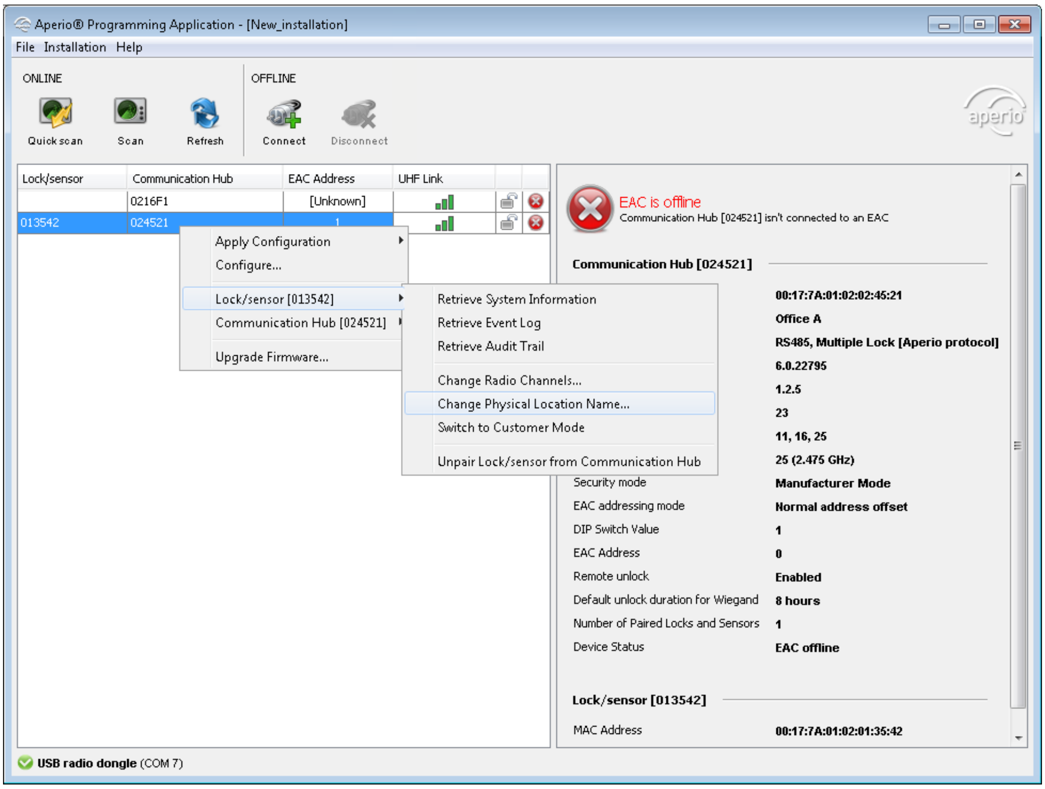
[DIP Switch]
1
2
3
4
5
6
7
8
9
10
11

2) Select the address and click *OK*.

Change physical location name – communication hub/lock/sensor

This function applies to both communication hubs and locks/sensors. In the example below the physical location name is changed for a lock/sensor.

1) Right-click and select *Lock/sensor – Change physical location name...*



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521	1	

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

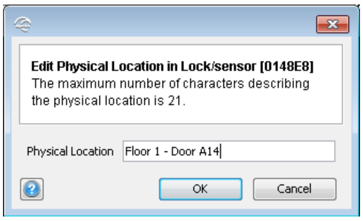
	00:17:7A:01:02:02:45:21
	Office A
	RS485, Multiple Lock [Aperio protocol]
	6.0.22795
	1.2.5
	23
	11, 16, 25
	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

MAC Address	00:17:7A:01:02:01:35:42

USB radio dongle (COM 7)

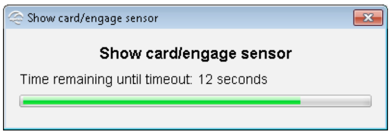
2) Enter a description that clearly identifies the lock position and click *OK*.



Edit Physical Location in Lock/sensor [0148E8]
The maximum number of characters describing the physical location is 21.

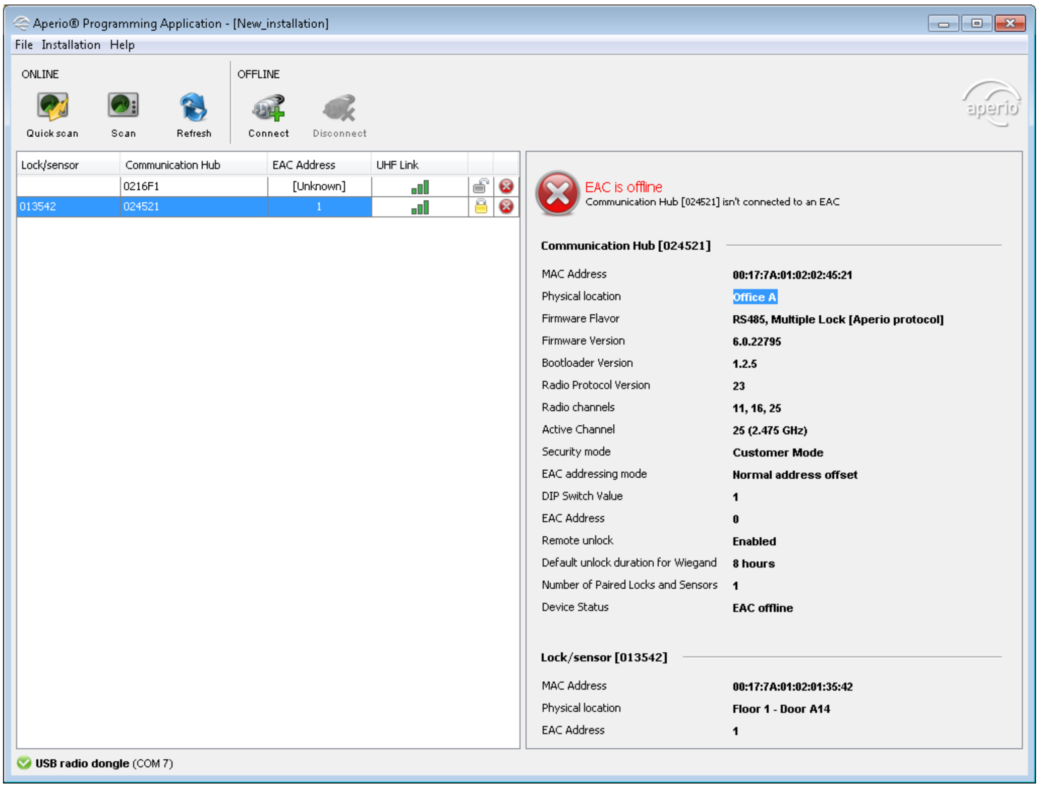
Physical Location: Floor 1 - Door A14

3) For a communication hub the information is updated immediately. If you change the physical location name for a lock/sensor you will be prompted to hold the credential at the lock, or engage the magnet for the sensor.



Show card/engage sensor
Time remaining until timeout: 12 seconds

Result: After successful reading a progress bar shows the download. After update the new location name can be found in the Lock/sensor section on the lower right side of the installation view.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521	1	

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

MAC Address	00:17:7A:01:02:02:45:21
Physical location	Office A
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.0.22795
Bootloader Version	1.2.5
Radio Protocol Version	23
Radio channels	11, 16, 25
Active Channel	25 (2.475 GHz)
Security mode	Customer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

MAC Address	00:17:7A:01:02:01:35:42
Physical location	Floor 1 - Door A14
EAC Address	1

USB radio dongle (COM 7)

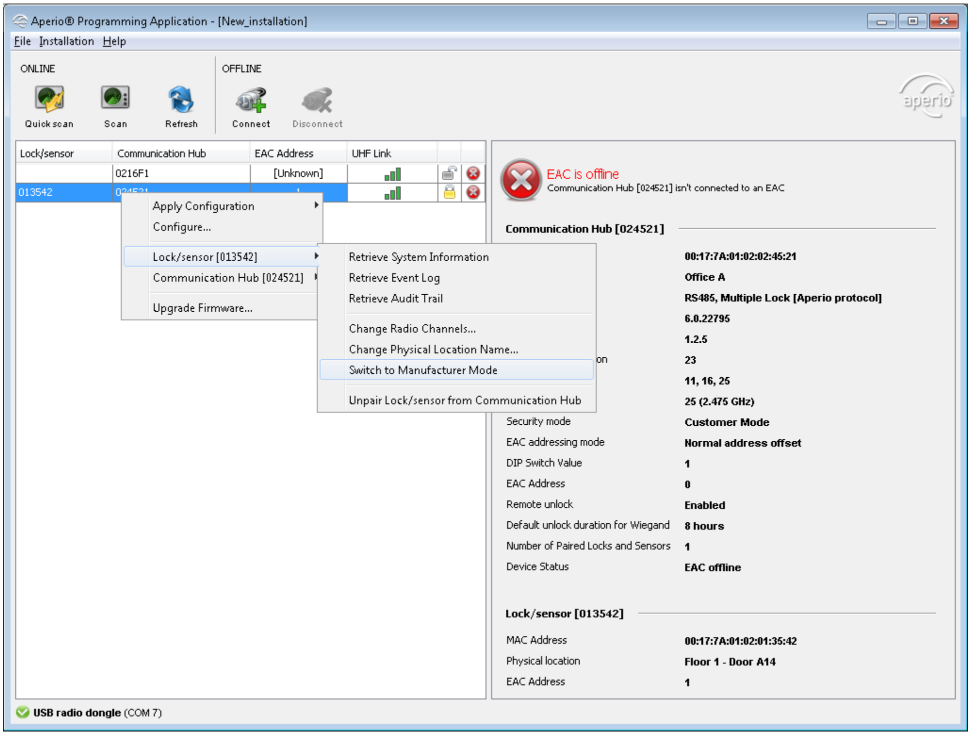
Change the Security Mode

Secure communication is normally set during first configuration of locks/sensors and communication hubs with the configure wizard. Security mode is also accessible through the right-click menu. During normal operation the security mode should not be altered. However, if the hardware must be sent to the factory for service or repair purposes, the security mode must be set to manufacturer mode before service.

Explanation of symbols:

🔒	*Customer mode*	Lock is using secure radio communication with the customer encryption key.
🔓	*Manufacturer mode*	Lock is using insecure radio communication with the default encryption key.
⊗	*Conflicting mode*	The modes in the lock/sensor and the communication hub are not the same.

1) Right-click the lock/sensor and select *Switch to Customer Mode/Switch to Manufacturer mode*.



Lock/sensor	Communication Hub	EAC Address	UHF Link		
	0216F1	[Unknown]		🔓	⊗
013542	024521	1		🔒	⊗

EAC is offline
Communication Hub [024521] isn't connected to an EAC

Communication Hub [024521]

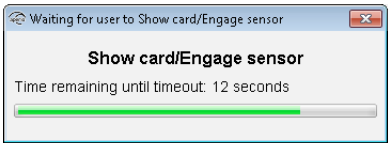
	00:17:7A:01:02:02:45:21
	Office A
	RS485, Multiple Lock [Aperio protocol]
	6.0.22795
	1.2.5
on	23
	11, 16, 25
	25 (2.475 GHz)
Security mode	Customer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	1
Device Status	EAC offline

Lock/sensor [013542]

MAC Address	00:17:7A:01:02:01:35:42
Physical location	Floor 1 - Door A14
EAC Address	1

USB radio dongle (COM 7)

2) Hold the credential at the lock, or engage the magnet for the sensor.

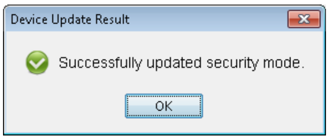


Show card/Engage sensor

Time remaining until timeout: 12 seconds

3) A progress bar shows that the transfer is being performed.

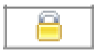
4) If the encryption key is successfully loaded you get a message that states "Successfully updated security mode". Click OK.



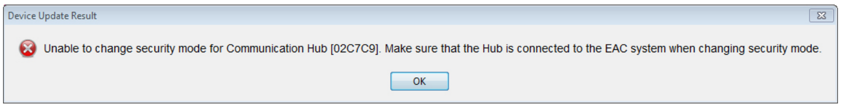
Device Update Result

Successfully updated security mode.

Result: Check the lock symbol at the right side of the lock to see that the lock has been set to Customer mode/Manufacturer mode.



AH40 communication hubs must be connected to an EAC system to accept change of security mode. If not so, the following error message is shown:



Device Update Result

Unable to change security mode for Communication Hub [02C7C9]. Make sure that the Hub is connected to the EAC system when changing security mode.

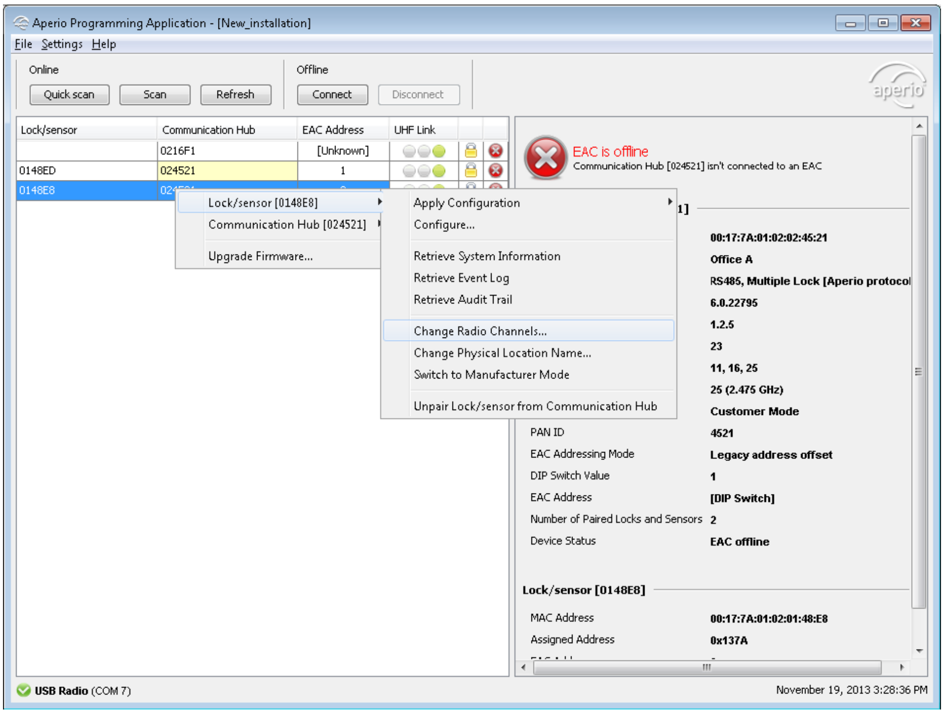
Change the radio channels

Changing the radio channels can be necessary if you experience interference between communication hubs, which can occur if many hubs are installed close to each other.

To use this function, you must have the *Show advanced settings* check box selected in *Preferences*, see section *"Preferences" on page* 9. Follow these steps to change the radio channel for the communication hub and lock/sensor:

Always change the radio channel in the locks/sensors before changing in the communication hub!

1) Select the lock/sensor in the scan result table. Right-click and select *Lock/sensor – Change radio channels*.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
0148ED	024521	1	
0148E8	024521		

EAC is offline
Communication Hub [024521] isn't connected to an EAC

	00:17:7A:01:02:02:45:21
	Office A
	RS485, Multiple Lock [Aperio protocol
	6.0.22795
	1.2.5
	23
	11, 16, 25
	25 (2.475 GHz)
	Customer Mode
PAN ID	4521
EAC Addressing Mode	Legacy address offset
DIP Switch Value	1
EAC Address	[DIP Switch]
Number of Paired Locks and Sensors	2
Device Status	EAC offline

Lock/sensor [0148E8]

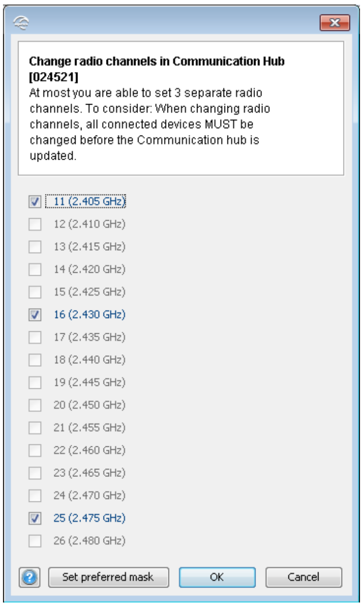
MAC Address	00:17:7A:01:02:01:48:E8
Assigned Address	0x137A

USB Radio (COM 7)

November 19, 2013 3:28:36 PM

2) Uncheck any of the three currently used channels to be able to select other radio channels. Click *OK*.

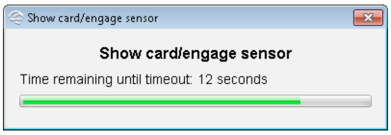
For the US market channel 26 is disabled.



Change radio channels in Communication Hub [024521]
At most you are able to set 3 separate radio channels. To consider: When changing radio channels, all connected devices MUST be changed before the Communication hub is updated.

☑ 11 (2.405 GHz)
☐ 12 (2.410 GHz)
☐ 13 (2.415 GHz)
☐ 14 (2.420 GHz)
☐ 15 (2.425 GHz)
☑ 16 (2.430 GHz)
☐ 17 (2.435 GHz)
☐ 18 (2.440 GHz)
☐ 19 (2.445 GHz)
☐ 20 (2.450 GHz)
☐ 21 (2.455 GHz)
☐ 22 (2.460 GHz)
☐ 23 (2.465 GHz)
☐ 24 (2.470 GHz)
☑ 25 (2.475 GHz)
☐ 26 (2.480 GHz)

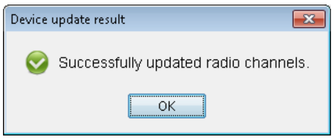
3) Hold the credential at the lock, or engage the magnet for the sensor to change radio channels.



Show card/engage sensor

Time remaining until timeout: 12 seconds

Result: A progress bar shows that the update is being performed. The *Device update result* dialog box shows the result of the update when it has been performed.

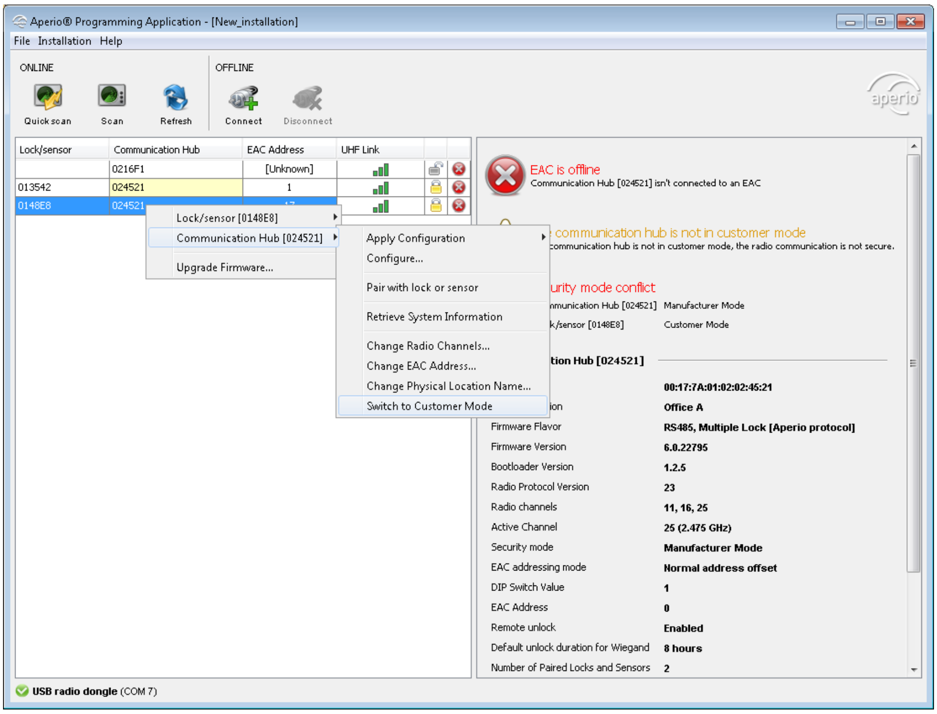


Successfully updated radio channels.

4) Repeat this procedure for all locks/sensors connected to the current communication hub.

Recommendation: Although it is possible to set different channels to locks/sensors paired with one hub, it is preferable to use the same three channels for all locks/sensors on that communication hub in order to create a more stable radio connection. Communication problems occur more likely between closely installed hubs than between closely installed locks/sensors paired with one hub.

5) Finally, change the radio channel for the communication hub: Right-click and select *Communication Hub – Change radio channels*.



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0216F1	[Unknown]	
013542	024521	1	
0148E8	024521		

EAC is offline
Communication Hub [024521] isn't connected to an EAC

communication hub is not in customer mode
communication hub is not in customer mode, the radio communication is not secure.

urity mode conflict

nmunication Hub [024521]	Manufacturer Mode
k/sensor [0148E8]	Customer Mode

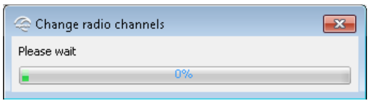
tion Hub [024521]

	00:17:7A:01:02:02:45:21
ion	Office A
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.0.22795
Bootloader Version	1.2.5
Radio Protocol Version	23
Radio channels	11, 16, 25
Active Channel	25 (2.475 GHz)
Security mode	Manufacturer Mode
EAC addressing mode	Normal address offset
DIP Switch Value	1
EAC Address	0
Remote unlock	Enabled
Default unlock duration for Wiegand	8 hours
Number of Paired Locks and Sensors	2

USB radio dongle (COM 7)

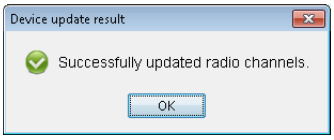
6) Uncheck any of the three currently used channels to be able to select the same radio channels as for the lock/sensor. Click *OK*.

Result: A progress bar shows that the update is being performed. The Device update result dialog box shows the result of the update when it has been performed.



Change radio channels

Please wait



Device update result

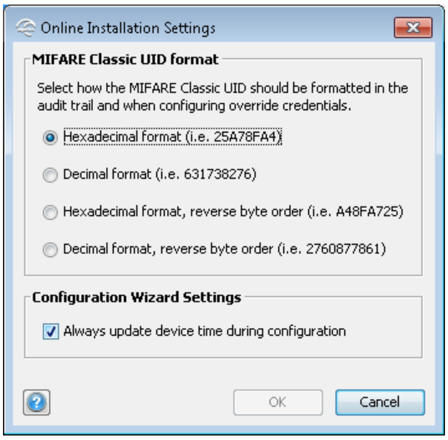
Successfully updated radio channels.

Setting the time of a lock

Follow these steps to set the time of a lock:

1) Select a lock in the installation view.

2) In the menu bar select *Installation – Online – Settings...* and check that the *Update device time during configuration* checkbox is checked.



Online Installation Settings

MIFARE Classic UID format

Select how the MIFARE Classic UID should be formatted in the audit trail and when configuring override credentials.

● Hexadecimal format (i.e. 25A78FA4)

○ Decimal format (i.e. 631738276)

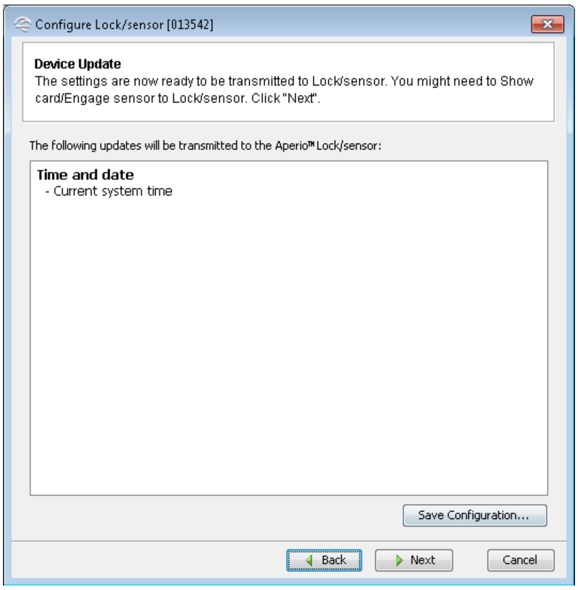
○ Hexadecimal format, reverse byte order (i.e. A48FA725)

○ Decimal format, reverse byte order (i.e. 2760877861)

Configuration Wizard Settings

☑ Always update device time during configuration

3) Close the *Online Installation Settings* view. Right-click and select *Lock/sensor-Configure*. Click *Next* repeatedly until you reach the *Device Update* window.



Configure Lock/sensor [013542]

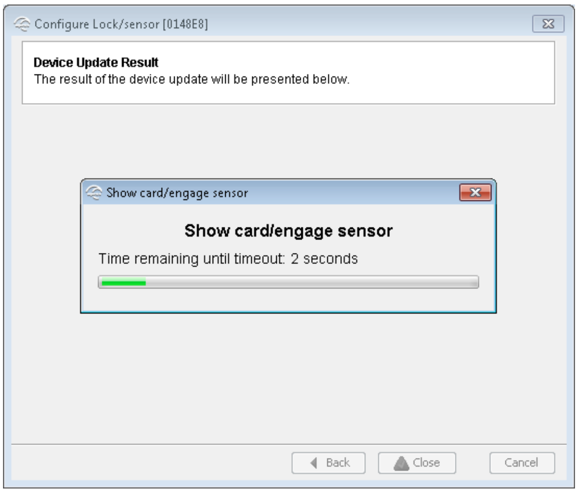
Device Update

The settings are now ready to be transmitted to Lock/sensor. You might need to Show card/Engage sensor to Lock/sensor. Click "Next".

The following updates will be transmitted to the Aperio™ Lock/sensor:

Time and date
- Current system time

4) Click *Next*.



Configure Lock/sensor [0148E8]

Device Update Result
The result of the device update will be presented below.

Show card/engage sensor

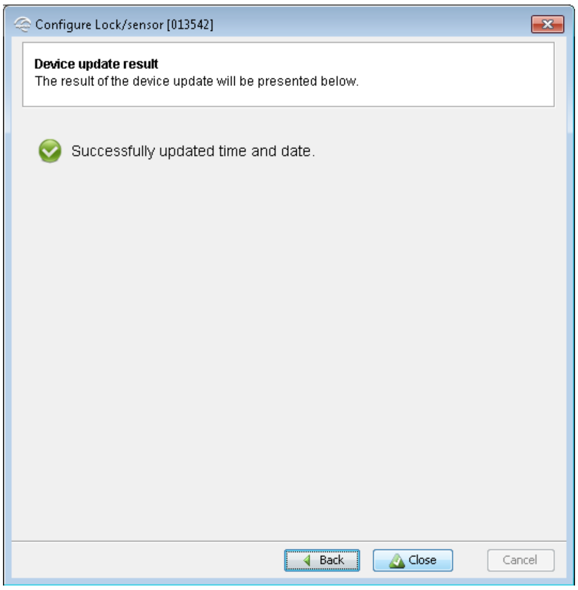
Show card/engage sensor

Time remaining until timeout: 2 seconds

5) Hold the credential at the lock, to update the time.

The time of the lock will now be automatically set each time you configure and update the device.

6) Click *Close* to exit the device update configuration.



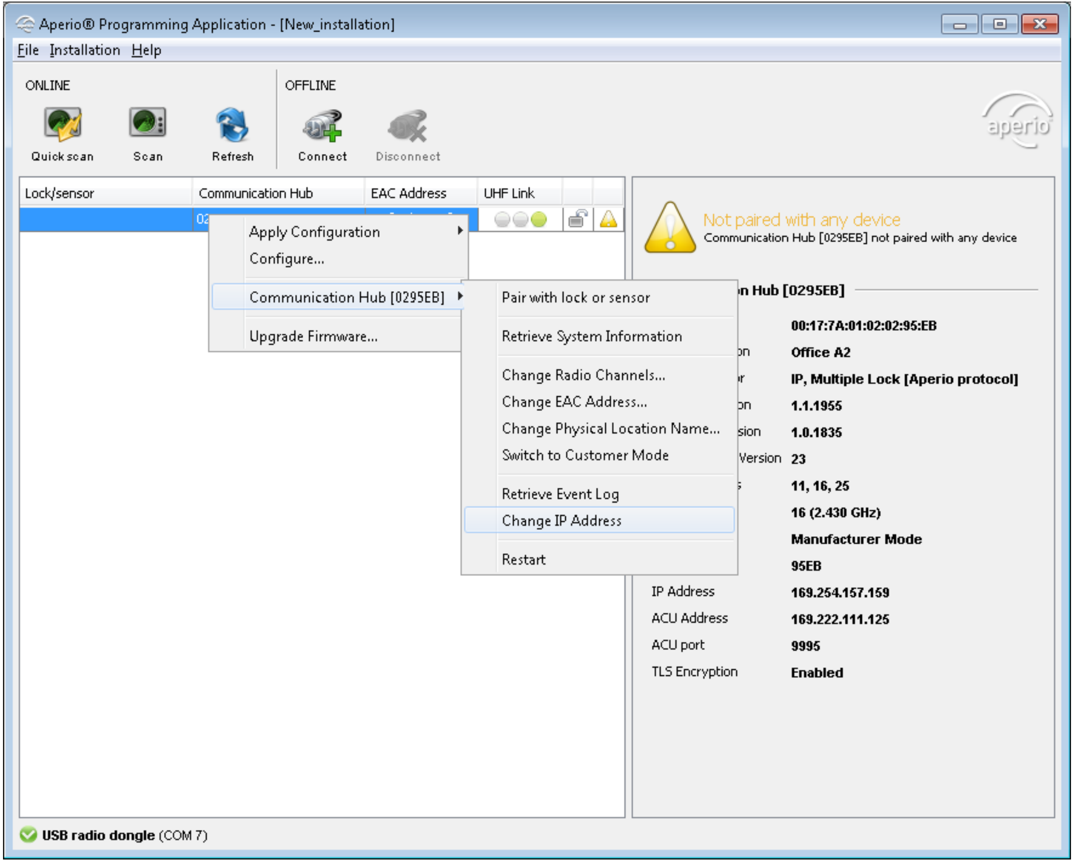
Configure Lock/sensor [013542]

Device update result
The result of the device update will be presented below.

Successfully updated time and date.

Change IP address (Communication hub AH40)

1) Right-click and select *Communication hub – Change IP Address*.



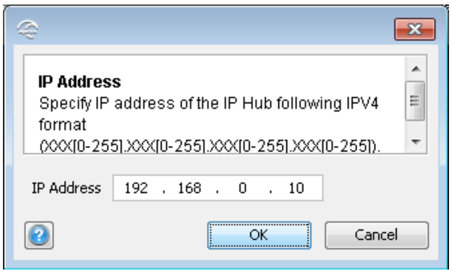
Not paired with any device
Communication Hub [0295EB] not paired with any device

n Hub [0295EB]

	00:17:7A:01:02:02:95:EB
on	Office A2
r	IP, Multiple Lock [Aperio protocol]
on	1.1.1955
sion	1.0.1835
Version	23
s	11, 16, 25
	16 (2.430 GHz)
	Manufacturer Mode
	95EB
IP Address	169.254.157.159
ACU Address	169.222.111.125
ACU port	9995
TLS Encryption	Enabled

USB radio dongle (COM 7)

2) Fill in the IP address of the IP communication hub. Click OK and the new IP address will be applied in the communication hub, and the IP communication will be restarted using the new IP address.



IP Address
Specify IP address of the IP Hub following IPV4 format
(XXX[0-255].XXX[0-255].XXX[0-255].XXX[0-255]).

IP Address 192 . 168 . 0 . 10

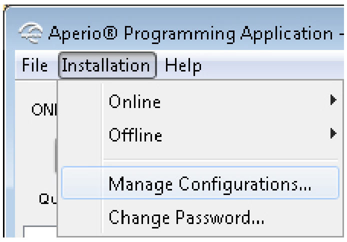
Managing configurations

The stored configurations made in the configuration wizard, can be exported to a file so that more than one Aperio Programming Application can share the same configuration information. When you import an exported configuration you add it to the local configuration storage and then you can apply that configuration to a lock/sensor or communication hub.

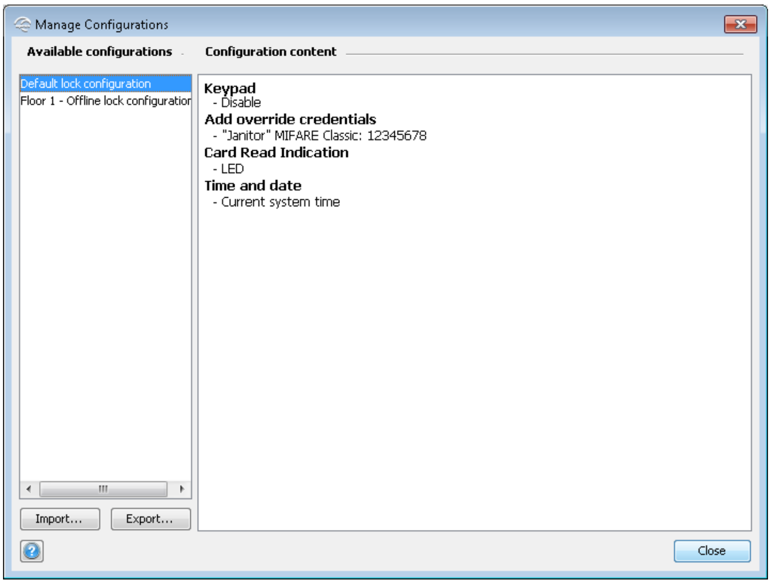
When you export a configuration, you cannot change the name of the configuration, only the file name holding the configuration information. Since configurations can be shared between different Aperio Programming Applications, it is preferable that a shared configuration (identified by its unique name) also has the same meaning on all Aperio Programming Applications. It is therefore advisable that you choose the name of the configuration wisely when you store the configuration.

Exporting Configuration

1) In the menu bar, select *Installation – Manage Configurations...*



2) Select the configuration that should be exported to file and click *Export*.



Available configurations

Default lock configuration
Floor 1 - Offline lock configuratior

Configuration content

Keypad
- Disable

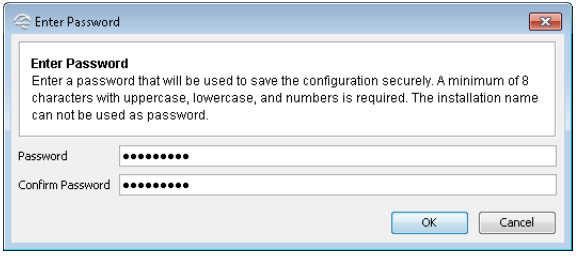
Add override credentials
- "Janitor" MIFARE Classic: 12345678

Card Read Indication
- LED

Time and date
- Current system time

3) Select the folder where you want to store the configuration, select a file name and click *Save*.

4) Choose a password that will be used when importing the particular configuration, confirm it and click *OK*.



Enter Password

Enter Password

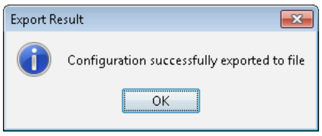
Enter a password that will be used to save the configuration securely. A minimum of 8 characters with uppercase, lowercase, and numbers is required. The installation name can not be used as password.

Password: •••••••••

Confirm Password: •••••••••

The password must contain at least 8 characters of which at least one upper and lower case character and a number.

Result:



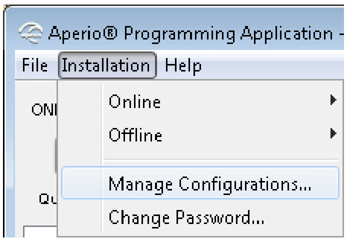
Export Result

Configuration successfully exported to file

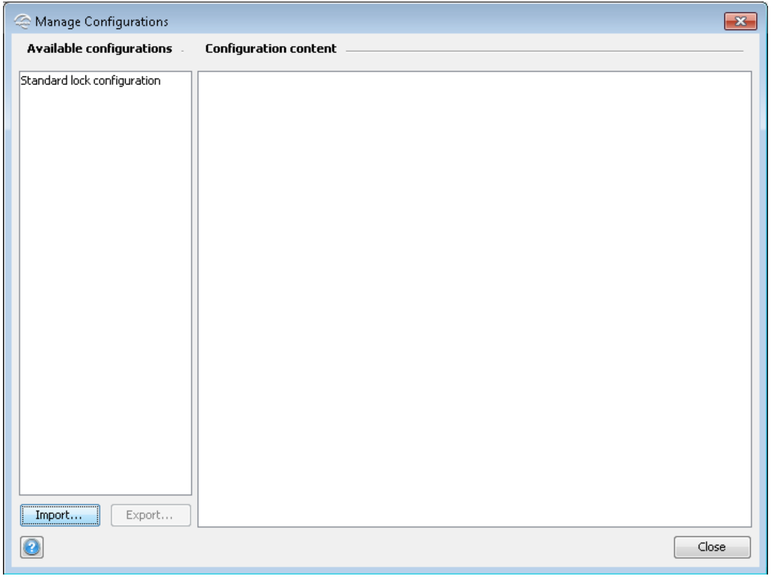
Importing Configuration

Importing a configuration takes a previously exported configuration and adds it to the local configuration storage.

1) In the menu bar, select *Manage Configurations...*

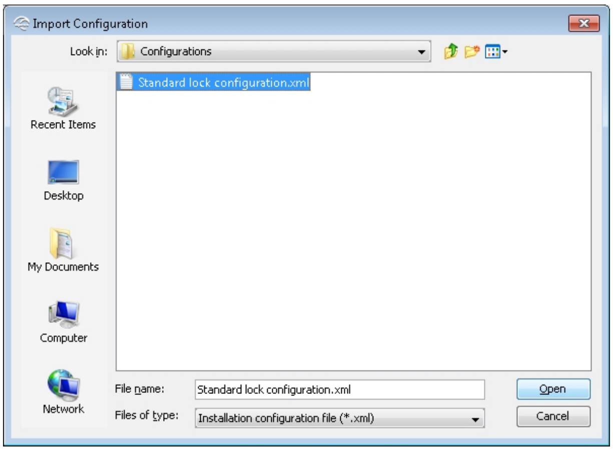


2) Click *Import...*



Standard lock configuration

3) Select a valid configuration XML-file and click *Open*.



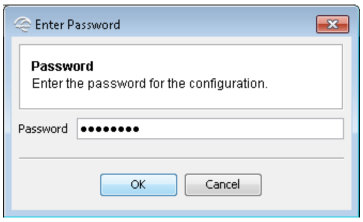
Look in: Configurations

Standard lock configuration.xml

File name: Standard lock configuration.xml

Files of type: Installation configuration file (*.xml)

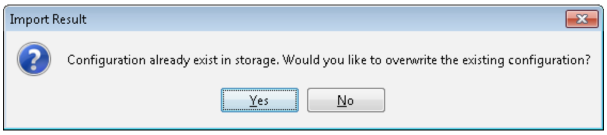
4) Enter the password and click *OK*.



Password
Enter the password for the configuration.

Password ••••••••

The configuration is identified by its name, not the name of the export file. When importing a configuration that already exists in the Programming Application you will be prompted if you want to replace the existing configuration.

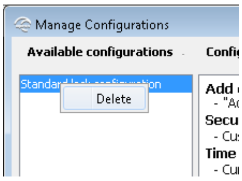


Import Result

Configuration already exist in storage. Would you like to overwrite the existing configuration?

Deleting configuration

In the *Manage Configurations* view you can also delete existing configurations: Right-click the configuration and select *Delete*.



Upgrade of communication hub/lock/sensor firmware

This chapter describes how to upgrade communication hubs and locks/sensors with a new firmware. The upgrade procedure will be executed only for the selected communication hub or lock/sensor, depending on the content of the firmware. The firmware file only contains firmware applicable to either a communication hub or a lock/sensor.

Always upgrade the communication hub before upgrading the locks/sensors. The reason is that communication hubs should always support older lock/sensor firmware but the opposite may not always be possible.

When upgrading AH30 communication hubs that use the DIP switch for EAC addressing, always check that the DIP switch is set to the correct EAC address. If DIP 5 (Pairing mode) is active by mistake, an upgrade will result in that the communication hub starts using a different EAC address.

When upgrading AH40 communication hubs to the latest firmware, Ethernet can be used to download the new firmware, provided that the AH40 communication hub IP address and other network settings has been correctly set up.

After firmware upgrade of all communication hubs versions always perform a *Rescan* to ensure that the Aperio Programming Application is sync with any new feature in the upgraded communication hub.

Upgrading

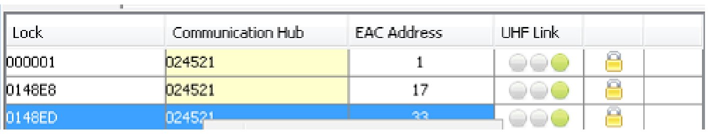
No sanity check is done by the Programming Application before the firmware download starts. Applying an older firmware than installed can cause the hardware to malfunction.

The Programming Application performs a check of firmware and lock so that the firmware always match the hardware. A C100 afw file will only be used with cylinder locks. An E100 afw file will only be used with escutcheon locks etc.

All firmware included in the afw file should be downloaded to hardware. Canceling the upgrade process or partly upgrading the hardware can cause malfunction.

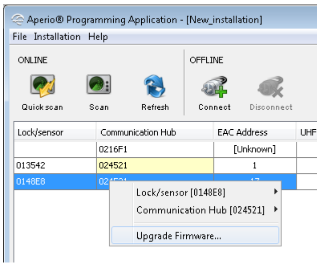
1) Ensure that you are using the latest version of the Aperio Programming Application. If not install the latest version.

2) Check on the UHF Link indicator that the signal strength indicator is good enough to be able to perform an upgrade (green or yellow). If you have bad signal strength (red) the Programming Application will not enable the upgrade function.



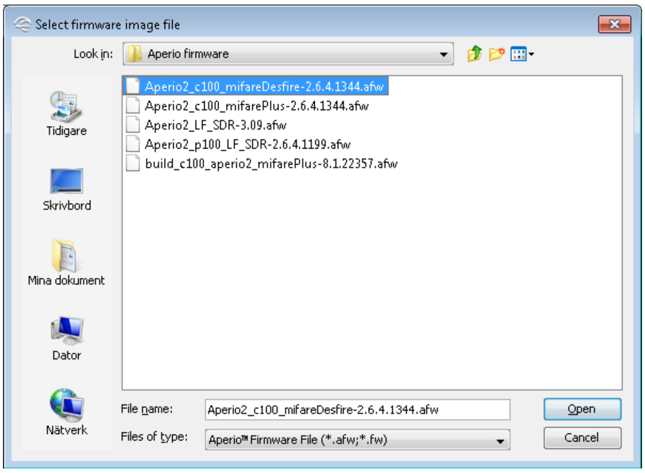
Lock	Communication Hub	EAC Address	UHF Link		
000001	024521	1	○○●		
0148E8	024521	17	○○●		
0148ED	024521	33	○○●		

3) Right-click on the communication hub/lock/sensor in the Installation view and select *Upgrade Firmware*.



Lock/sensor	Communication Hub	EAC Address	UHF
	0216F1	[Unknown]	
013542	024521	1	
0148E8	02	17	

4) Select the firmware file (.afw/.fw file) and click *Open*.



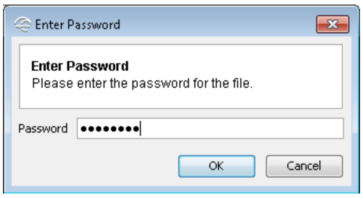
Look in: Aperio firmware

Aperio2_c100_mifareDesfire-2.6.4.1344.afw
Aperio2_c100_mifarePlus-2.6.4.1344.afw
Aperio2_LF_SDR-3.09.afw
Aperio2_p100_LF_SDR-2.6.4.1199.afw
build_c100_aperio2_mifarePlus-8.1.22357.afw

File name: Aperio2_c100_mifareDesfire-2.6.4.1344.afw

Files of type: Aperio™ Firmware File (*.afw;*.fw)

5) Enter the password supplied with the firmware.

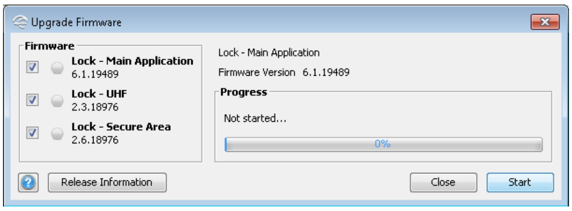


Enter Password

Enter Password
Please enter the password for the file.

Password ••••••••

Result: The firmware upgrade window is shown, with a list of the units that may be upgraded. Depending on the firmware file, the list of firmware may vary. Two examples are shown below. (Click *Release Info* to get more information of firmware file.)

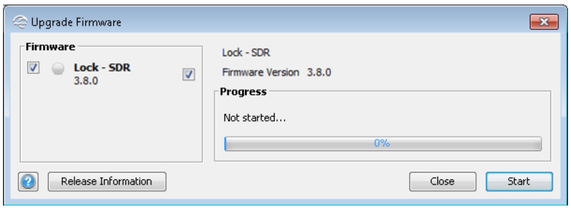


Upgrade Firmware

Firmware
☑ **Lock - Main Application** 6.1.19489
☑ **Lock - UHF** 2.3.18976
☑ **Lock - Secure Area** 2.6.18976

Lock - Main Application
Firmware Version 6.1.19489

Progress
Not started...
0%



Upgrade Firmware

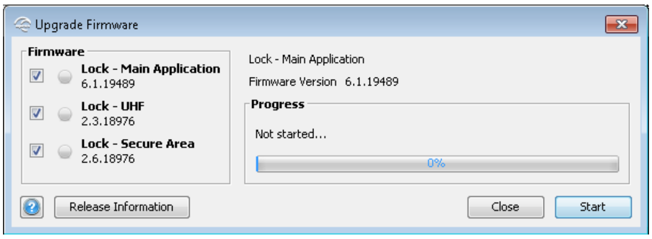
Firmware
☑ **Lock - SDR** 3.8.0 ☑

Lock - SDR
Firmware Version 3.8.0

Progress
Not started...
0%

6) All firmware is selected to be downloaded by default.

Only uncheck firmware if site specific settings allow this. Existing old firmware in hardware combined with new firmware can cause malfunction.



Upgrade Firmware

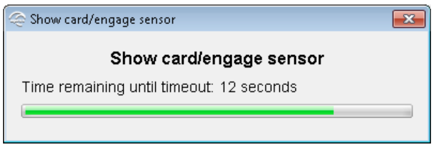
Firmware
☑ **Lock - Main Application** 6.1.19489
☑ **Lock - UHF** 2.3.18976
☑ **Lock - Secure Area** 2.6.18976

Lock - Main Application
Firmware Version 6.1.19489

Progress
Not started...
0%

7) Click *Start* to initiate the upgrade process.

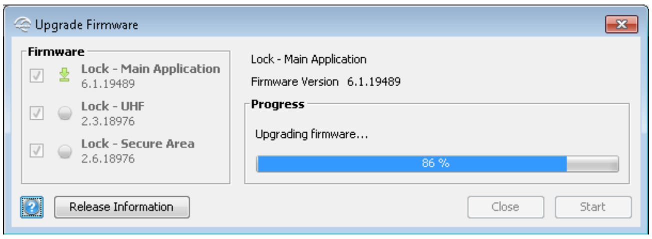
8) If you are upgrading a lock/sensor you will be prompted to hold a credential at the lock/engage sensor before the download starts.



Show card/engage sensor

Show card/engage sensor
Time remaining until timeout: 12 seconds

Result: The upgrade will start with the first firmware in the list. A green arrow to the left of the selected firmware will indicate the firmware is being upgraded and the firmware is downloaded.



Lock - Main Application

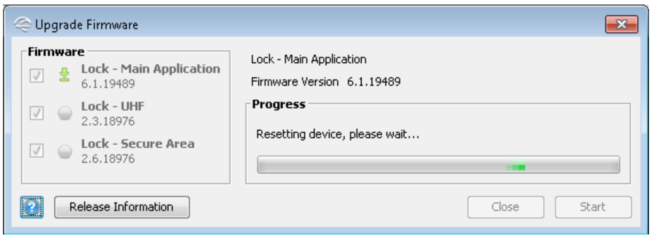
Firmware Version 6.1.19489

Progress

Upgrading firmware...

86 %

After finished download, the device resets.



Lock - Main Application

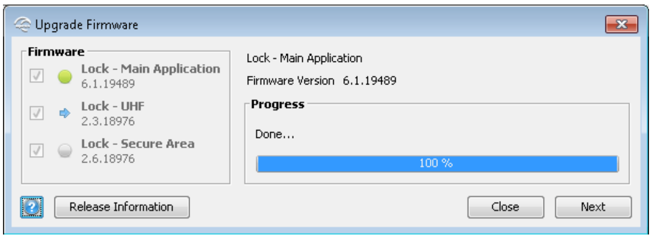
Firmware Version 6.1.19489

Progress

Resetting device, please wait...

9) Click *Next* to continue with the next firmware in the list.

Canceling the firmware upgrade process by clicking *Close* should be avoided. Existing old firmware in hardware combined with new firmware can cause malfunction.



Lock - Main Application

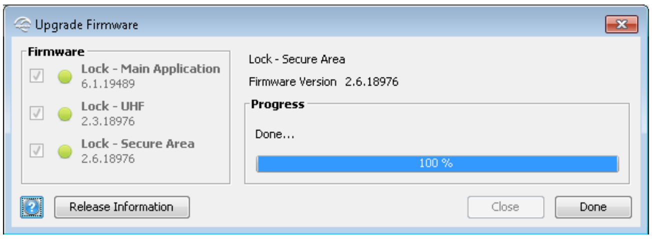
Firmware Version 6.1.19489

Progress

Done...

100 %

10) After all firmware is downloaded, click *Done*.



Lock - Secure Area

Firmware Version 2.6.18976

Progress

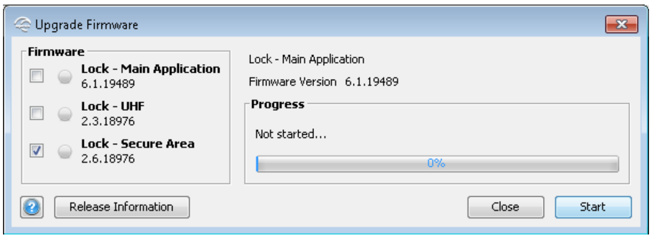
Done...

100 %

Upgrade failure

A failed update is typically due to bad radio conditions. The work around is to move the USB Radio closer to the communication hub and try update again.

1) Click *Save support information to file* if desired and click *OK* to close the error message.

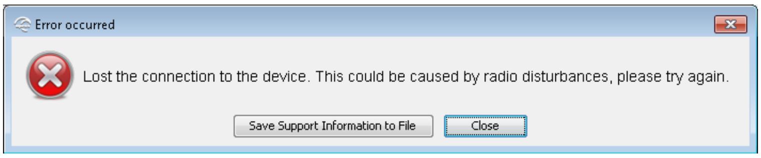


Upgrade Firmware

Firmware
- ☐ Lock - Main Application 6.1.19489
- ☐ Lock - UHF 2.3.18976
- ☑ Lock - Secure Area 2.6.18976

Lock - Main Application
Firmware Version 6.1.19489

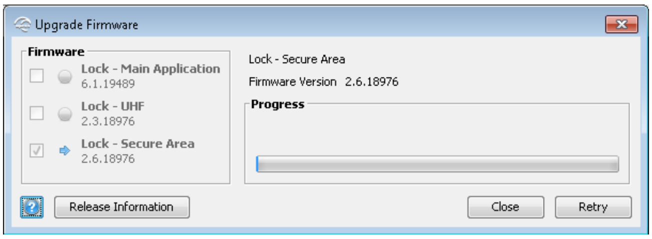
Progress
Not started...
0%



Error occurred

Lost the connection to the device. This could be caused by radio disturbances, please try again.

2) Click *Retry* to try the upgrade again.



Upgrade Firmware

Firmware
- ☐ Lock - Main Application 6.1.19489
- ☐ Lock - UHF 2.3.18976
- ☑ Lock - Secure Area 2.6.18976

Lock - Secure Area
Firmware Version 2.6.18976

Progress

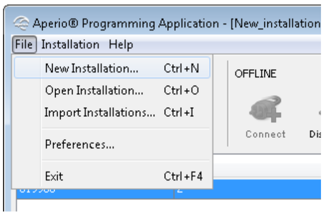
5 Programming Application Offline Functions

Opening/creating installations

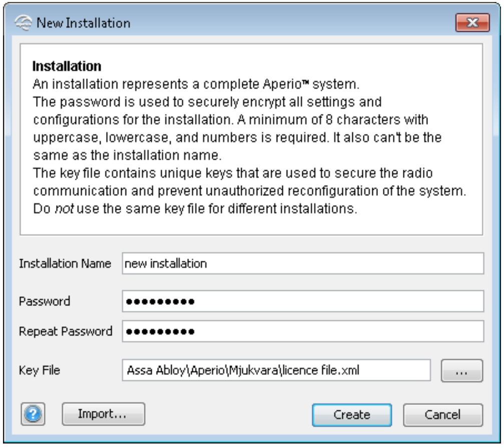
An installation is a password protected set of settings you need when you want to communicate with a lock. An installation is linked to an encryption file that is needed in order for the communication to work. (The encryption key file is provided by your local ASSA ABLOY company.)

1) Insert the USB Radio dongle and start the Aperio Programming application.

2) Select *File - New installation...* or *Open Installation...* in the Programming Application.


Aperio® Programming Application - [New_installation
File Installation Help
New Installation... Ctrl+N
Open Installation... Ctrl+O
Import Installations... Ctrl+I
Preferences...
Exit Ctrl+F4
OFFLINE
Connect
Di

3) Enter a name for the installation, a password matching the requirements and finally click the button in the Key file field to add the Encryption key.



New Installation

Installation
An installation represents a complete Aperio™ system.
The password is used to securely encrypt all settings and configurations for the installation. A minimum of 8 characters with uppercase, lowercase, and numbers is required. It also can't be the same as the installation name.
The key file contains unique keys that are used to secure the radio communication and prevent unauthorized reconfiguration of the system. Do *not* use the same key file for different installations.

Installation Name: new installation
Password: •••••••••
Repeat Password: •••••••••
Key File: Assa Abloy\Aperio\Mjukvara\licence file.xml

4) Click *Create*.

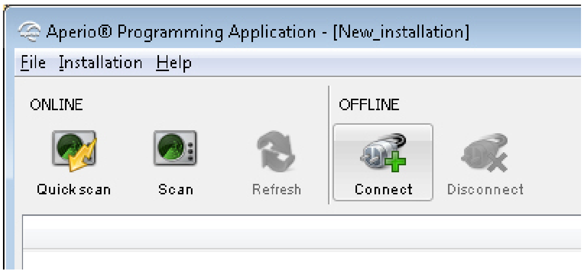
Importing Existing Installations

This procedure is equal as for Aperio Online. See section "*Import Existing Installations" on page 14.*

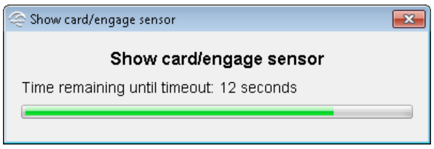
Connecting to an offline lock

Follow these steps to connect to an offline lock:

1) Click *Connect* in the Offline section of the menu bar.



2) Hold the radio activation card at the lock (or remove and reinsert the battery).

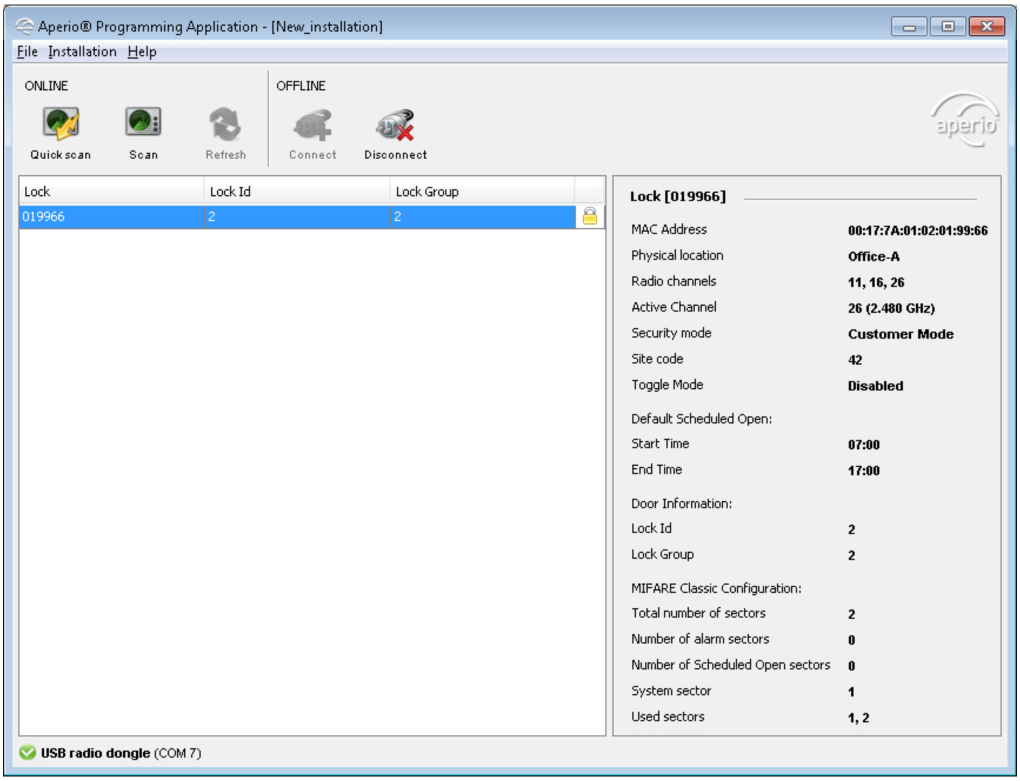


Show card/engage sensor

Show card/engage sensor

Time remaining until timeout: 12 seconds

Result: Detailed information is downloaded and the Programming application connects to the lock.



Aperio® Programming Application - [New_installation]

Lock	Lock Id	Lock Group
019966	2	2

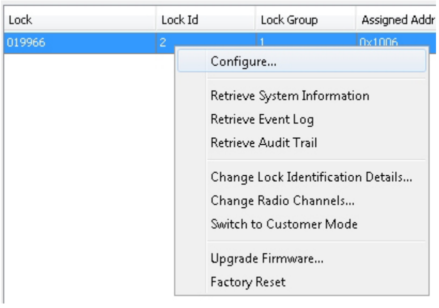
Lock [019966]

MAC Address	**00:17:7A:01:02:01:99:66**
Physical location	**Office-A**
Radio channels	**11, 16, 26**
Active Channel	**26 (2.480 GHz)**
Security mode	**Customer Mode**
Site code	**42**
Toggle Mode	**Disabled**
Default Scheduled Open:	
Start Time	**07:00**
End Time	**17:00**
Door Information:	
Lock Id	**2**
Lock Group	**2**
MIFARE Classic Configuration:	
Total number of sectors	**2**
Number of alarm sectors	**0**
Number of Scheduled Open sectors	**0**
System sector	**1**
Used sectors	**1, 2**

USB radio dongle (COM 7)

Configure function – Wizard

1) Select a lock in the scan result table, right-click and select *Configure...*

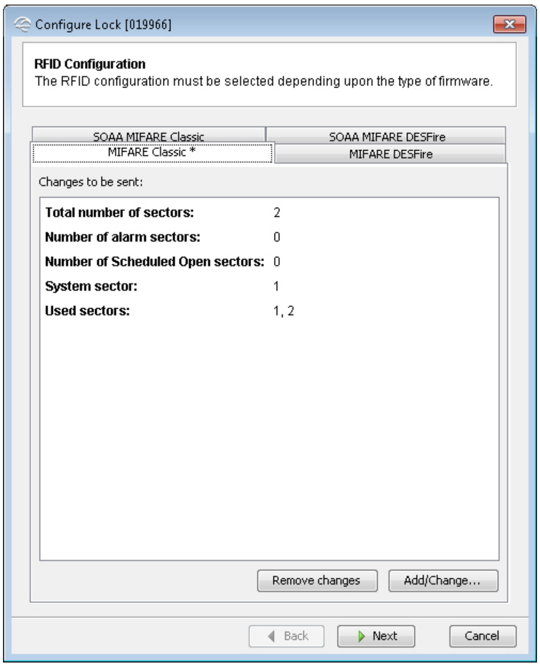


2) Click *Next* after completion of each dialog in the Configuration Wizard.

The following sections describe each window in the wizard.

RFID configuration

Select the tab depending upon the lock type. Only one type of configuration can be sent to the Lock. Click *Add/Change...* to enter the settings for each card format.



RFID Configuration
The RFID configuration must be selected depending upon the type of firmware.

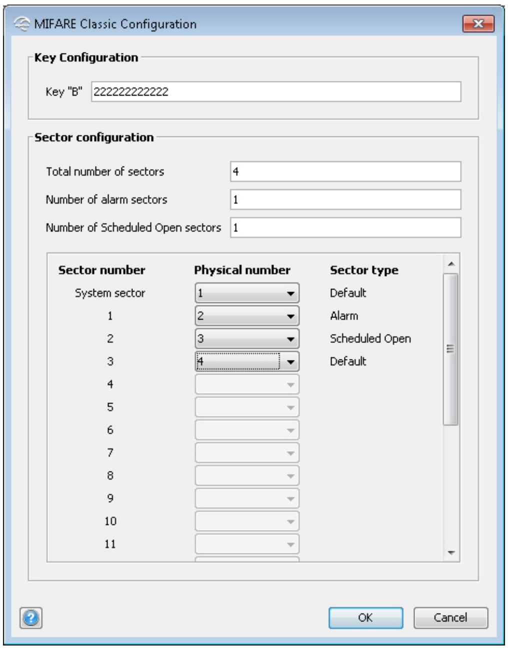
Changes to be sent:

Total number of sectors:	2
Number of alarm sectors:	0
Number of Scheduled Open sectors:	0
System sector:	1
Used sectors:	1, 2

MIFARE Classic configuration

MIFARE Classic configurations is a part of the Lock-Unit setup information that describes which MIFARE sectors are to be used by the Aperio Offline application. This configuration screen allows the user to specify a MIFARE 'B' key and configure the MIFARE-sector usage (system sector, alarm sector, scheduled open sector).

If MIFARE RFID configuration is done wrong, the lock may become inoperable.



MIFARE Classic Configuration

Key Configuration

Key "B" 222222222222

Sector configuration

Total number of sectors 4

Number of alarm sectors 1

Number of Scheduled Open sectors 1

Sector number	Physical number	Sector type
System sector	1	Default
1	2	Alarm
2	3	Scheduled Open
3	4	Default
4		
5		
6		
7		
8		
9		
10		
11		

Key configuration:

- **MIFARE key B:** Enter the 6 byte long hexadecimal MIFARE Classic Key B that applies for the user cards in your installation. Example: AABBCC112233.

Sector configuration:

- **Total number of sectors:** Enter the total number of sectors to be used on the card.
- **Number of alarm sectors:** Enter the number of alarm sectors reserved on access cards used on the particular site.
- **Number of scheduled open sectors:** Enter number of scheduled open sectors reserved on access cards used on the particular site.

After adding the number of sector used, click the *Physical number* drop down menu to select/change a physical number for each sector.

Physical numbers not used are free to be used by other applications.

System limitation

The sector configuration settings affect the number of lock groups that can be used (see section *"Change lock identification details" on page 98*).

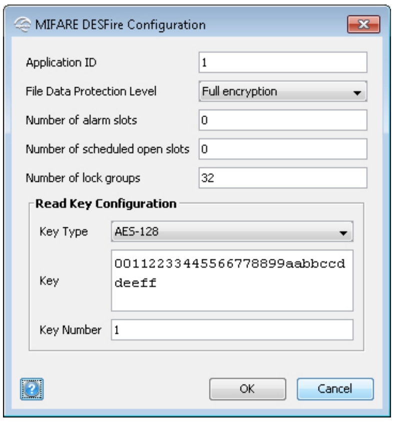
Plan your sector configuration with the following limitations in mind:

	MIFARE Classic 1K	MIFARE Classic 4K
Max lock units	65536	65536
Max lock groups	1344	5088
Max alarms	84	420

Having max lock groups means no alarms and vice versa since they share the same storage space on the credential.
It is up to the system owner to ensure that the appropriate number of sectors needed to represent all doors is reserved on all user credentials in the system.

It is recommended to reserve extra sectors not reserved for alarms/schedules, in order to obtain space for lock group addressing. Each free sector allows 96 lock groups (MIFARE Classic 1K card).

MIFARE DESFire Configuration



Application ID: 1
File Data Protection Level: Full encryption
Number of alarm slots: 0
Number of scheduled open slots: 0
Number of lock groups: 32

Read Key Configuration
Key Type: AES-128
Key: 00112233445566778899aabbccddeeff
Key Number: 1

- **Application ID:** Identification number for the Aperio Offline application on the MIFARE DESFire cards used in the system. A MIFARE DESFire card can have up to 32 applications. Application ID:s range from 0 to 16777215.
- **File Data Protection Level:** Security level for the communication between lock and card. Choose one of the two options (Data Authenticity by MAC, Full Encryption) depending on how the cards used in the system are configured.
- **Number of alarm slots:** Numeric value representing number of alarm slots on access cards used in the system.
- **Number of scheduled open slots:** Numeric value representing number of scheduled open slots on access cards used in the system.
- **Number of lock groups:** Numeric value representing maximum number of allowed lock groups on access cards used in the system.
- **Key Type:** Choose one of the three options (2K3DES, 3K3DES, AES-128) depending on the cryptographic algorithm used to read/write data from/to the card. Type the key value in hexadecimal. 2K3DES and AES-128 are 16 byte keys. 3K3DES is a 24 byte key.

- **Key:** MIFARE DESFire key that applies for the user cards in your installation in HEX format. Example: 00112233445566778899aabbccddeeff.
- **Key Number:** Each application can use up to 14 keys. Key 0 is always the Application's Master Key. Type here which key number that is used for the Aperio Offline application on the MIFARE DESFire cards. Key numbers range from 0 to 13.

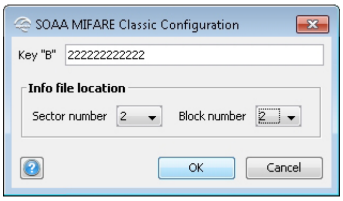
System limitation
It is up to the system owner to assure that there is space enough on the access cards used for the actual system configuration. Possible configurations are dependent on the size of the MIFARE DESFire EV1 cards used in the system and if they are used for other applications than Aperio Offline.

Plan your sector configuration with the following limitations in mind:

	MIFARE DESFire 2K	MIFARE DESFire 4K	MIFARE DESFire 8K
Max lock groups	4000	8096	16288
Max alarm slots	250	506	1018
Max scheduled open slots	500	1012	2036

Having max lock groups means no alarms and vice versa since they share the same storage space on the credential.

SOAA MIFARE Classic configuration



SOAA MIFARE Classic Configuration

Key "B" 222222222222

Info file location

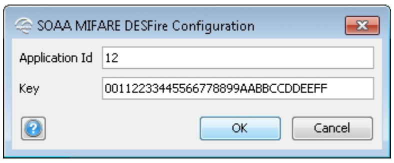
Sector number 2

Block number 2

- **MIFARE key B:** Enter the 6 byte long hexadecimal MIFARE Classic Key B that applies for the user cards in your installation. Example: AABBCC112233.

Info file location:
- **Sector number:** Start sector used for the SOAA infomation file, in the range of 0-39.
- **Block number:** Start block for the SOAA information file in the used sector. 0-2 or 0-14 for sectors 32 and higher.

SOAA MIFARE DESFire Configuration



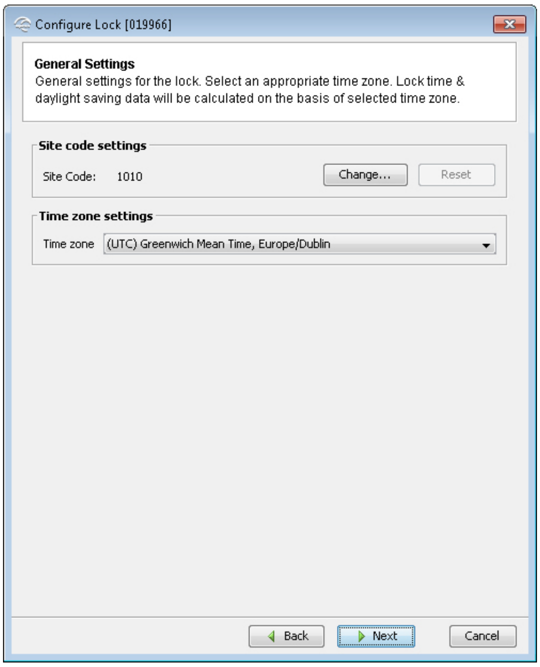
SOAA MIFARE DESFire Configuration

Application Id: 12

Key: 00112233445566778899AABBCCDDEEFF

- **Application ID:** Identification number for the Aperio Offline application on the MIFARE DESFire cards used in the system. A MIFARE DESFire card can have up to 32 applications. Application ID:s range from 0 to 16777215.
- **Key:** MIFARE DESFire key that applies for the user cards in your installation in HEX format. Example: 00112233445566778899aabbccddeeff.

General settings



Configure Lock [019966]

General Settings

General settings for the lock. Select an appropriate time zone. Lock time & daylight saving data will be calculated on the basis of selected time zone.

Site code settings

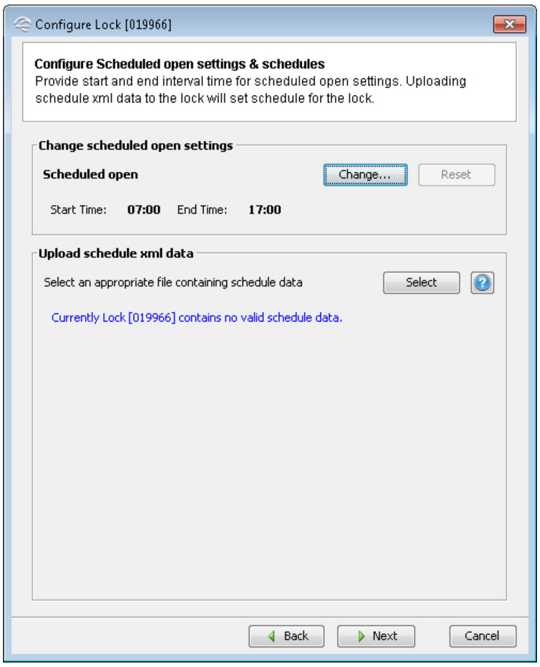
Site Code: 1010

Time zone settings

Time zone: (UTC) Greenwich Mean Time, Europe/Dublin

- **Site code settings:** Each site has a unique code number that all credentials within the system share. It is a mandatory field on the screen where the user is allowed to enter only 9-10 (4 bytes max) digit numeric values.
- **Time zone settings:** Select the time zone where the access system is located.

Scheduled Open & Schedule data



Configure Scheduled open settings & schedules
Provide start and end interval time for scheduled open settings. Uploading schedule xml data to the lock will set schedule for the lock.

Change scheduled open settings

Scheduled open

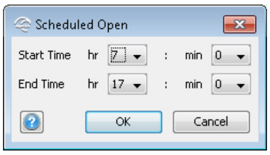
Start Time: **07:00** End Time: **17:00**

Upload schedule xml data

Select an appropriate file containing schedule data

Currently Lock [019966] contains no valid schedule data.

Change Scheduled Open settings



Start Time hr 7 : min 0

End Time hr 17 : min 0

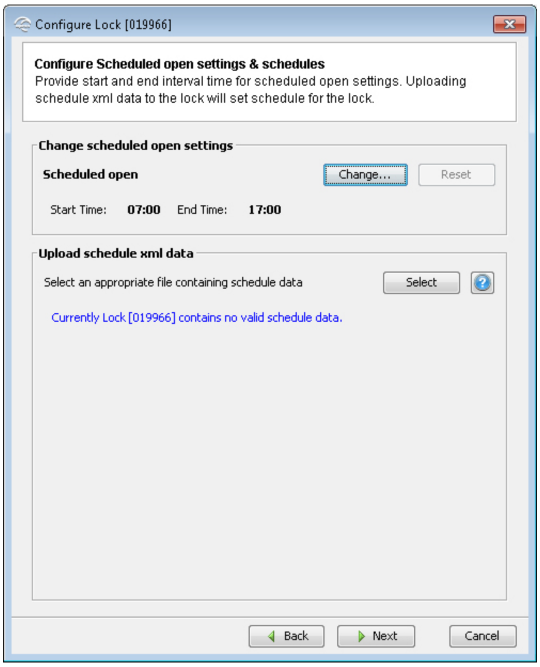
- **Start time:** Start time for when the lock can be activated for scheduled open (For when access cards with scheduled open functionality can set the lock to be open).
- **End time:** End time for when the lock responds to scheduled open attempts. It is also the time when the lock goes back to locked state after being scheduled open unlocked.

The scheduled open function has several options, please refer to the Aperio Offline System Description manual for more details.

Scheduled Open and Schedule data settings are not applicable to SOAA products.

Upload schedule data

With this function schedules are enabled in the lock. The schedules for the specific access system are specified in an XML-file.



Configure Lock [019966]

Configure Scheduled open settings & schedules

Provide start and end interval time for scheduled open settings. Uploading schedule xml data to the lock will set schedule for the lock.

Change scheduled open settings

Scheduled open

Start Time: **07:00** End Time: **17:00**

Upload schedule xml data

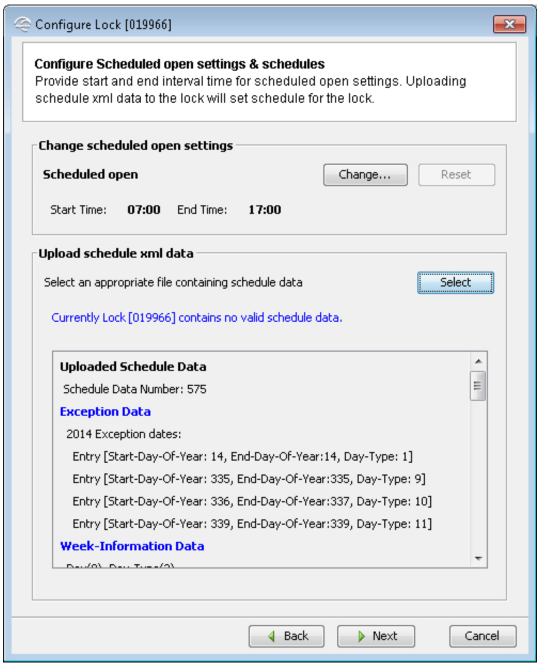
Select an appropriate file containing schedule data

Currently Lock [019966] contains no valid schedule data.

1) Click *Select* and then open to select XML with schedule data from your system/network to be uploaded.

Schedule file selected should have data in correct format according to specified XML structure, see below.

2) Check that the schedule data is correct.



Configure Scheduled open settings & schedules
Provide start and end interval time for scheduled open settings. Uploading schedule xml data to the lock will set schedule for the lock.

Change scheduled open settings

Scheduled open

Start Time: **07:00** End Time: **17:00**

Upload schedule xml data

Select an appropriate file containing schedule data

Currently Lock [019966] contains no valid schedule data.

Uploaded Schedule Data
Schedule Data Number: 575
Exception Data
2014 Exception dates:
Entry [Start-Day-Of-Year: 14, End-Day-Of-Year:14, Day-Type: 1]
Entry [Start-Day-Of-Year: 335, End-Day-Of-Year:335, Day-Type: 9]
Entry [Start-Day-Of-Year: 336, End-Day-Of-Year:337, Day-Type: 10]
Entry [Start-Day-Of-Year: 339, End-Day-Of-Year:339, Day-Type: 11]
Week-Information Data

Schedule Data XML format

Follow these guidelines when creating XML-file for defining schedule data:

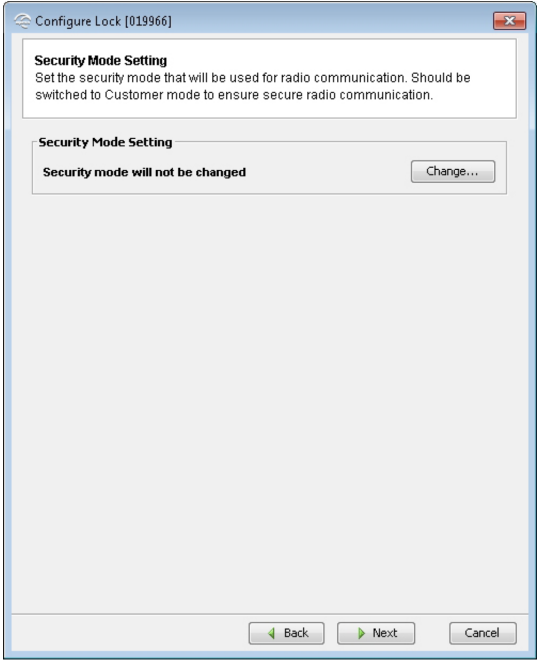
- File containing schedule data should be in XML format.
- Schedule data file should have xml extension (ex. schedule_data.xml).

Rules for Schedule data

Tag/Attribute Name	Rules
<year>(Exceptions)	Value should be greater than or equal to the current year.
<daytype>(Exceptions>>Year>>Entry)	Value should be in the range 0-63 (inclusive).
<startdate> & <enddate>(Exceptions>>Year>>Entry)	Values specified should be in YYYY-MM-DD format. <startdate> value should be less than or equal(in case of a single day exception) to <enddate> value. Year specified in <startdate> & <enddate> tags should always be same as the above <year> tag value.
daynumber(Weekdays>>Day)	Value specified should be in the range 0 (Mon) - 6 (Sun) inclusive.
daytype(Weekdays>>Day)	Value specified should be in the range 0-63 (inclusive).
<schedule>(Schedules)	Number value specified should be in the range 2-15 (inclusive). Type value should only be a numeric value.
<type>(Schedules>>schedule)	Only two type of schedules are allowed 0(Default access schedule), 1(Schedule open). There can be only one type="1" (Schedule open) schedule in the XML. There can be any number of type="0" (default Access) schedule in the XML.
<daytype>(Schedules>>schedule)	Value specified should be in the range 0-63 (inclusive).
<start-interval> & <end-interval>(Schedules>>schedule>>daytype)	Time should be specified in HH:MM 24 hour format. Data should always be entered in terms of quarter of the day. <start-interval> should signify start of the quarter time hence MM value should be one of these values (00,15,30,45). <end-interval> should signify end of the quarter time hence MM value should be one of these values (14,29,44,59).

The Aperio Programming Application F1-help contains a complete example of a Schedule data XML-file and XSD used.

Security Mode Settings



Configure Lock [019966]

Security Mode Setting

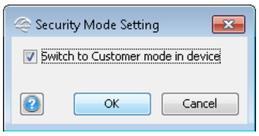
Set the security mode that will be used for radio communication. Should be switched to Customer mode to ensure secure radio communication.

Security Mode Setting

Security mode will not be changed

1) Click *Change* in the Security Mode Setting area if you want to change the security mode, or click *Next*.

2) To change to customer mode, click the check box and click OK.



Security Mode Setting

☑ Switch to Customer mode in device

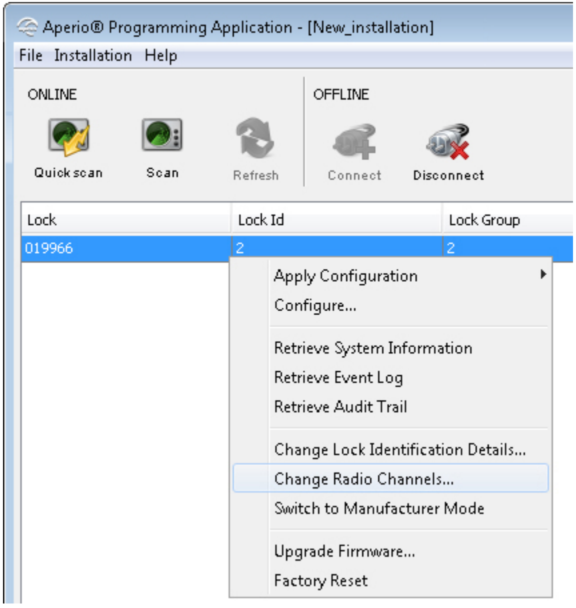
The default mode is Manufacturer mode , but you should always change it to Customer mode. If you change to Manufacturer mode the lock will no longer be using secure radio communication.

Change the radio channels

Changing the radio channel can be necessary if you experience interference between lock and USB Radio dongle.

To use this function, you must have the *Show advanced settings* checkbox selected in *Preferences*, see section *"Preferences" on page 9*. Follow these steps to change the radio channel for the communication hub and lock/sensor:

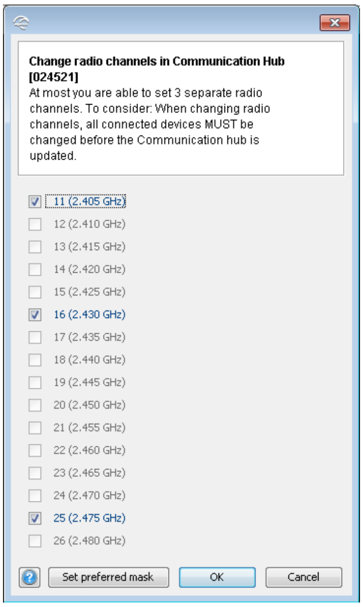
1) Select the lock in the scan result table. Right-click and select *Change radio channels...*



Lock	Lock Id	Lock Group
019966	2	2

2) Uncheck any of the three currently used channels to be able to select other radio channels. Click *OK*.

For the US market channel 26 is disabled.

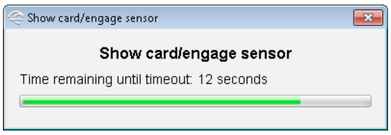


Change radio channels in Communication Hub [024521]

At most you are able to set 3 separate radio channels. To consider: When changing radio channels, all connected devices MUST be changed before the Communication hub is updated.

☑ 11 (2.405 GHz)
☐ 12 (2.410 GHz)
☐ 13 (2.415 GHz)
☐ 14 (2.420 GHz)
☐ 15 (2.425 GHz)
☑ 16 (2.430 GHz)
☐ 17 (2.435 GHz)
☐ 18 (2.440 GHz)
☐ 19 (2.445 GHz)
☐ 20 (2.450 GHz)
☐ 21 (2.455 GHz)
☐ 22 (2.460 GHz)
☐ 23 (2.465 GHz)
☐ 24 (2.470 GHz)
☑ 25 (2.475 GHz)
☐ 26 (2.480 GHz)

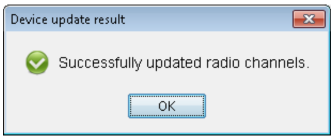
3) Hold the radio activation card at the lock (or remove and reinsert the battery) to perform the update.



Show card/engage sensor

Time remaining until timeout: 12 seconds

Result: A progress bar shows that the update is being performed. The Device update result dialog box shows the result of the update when it has been performed.



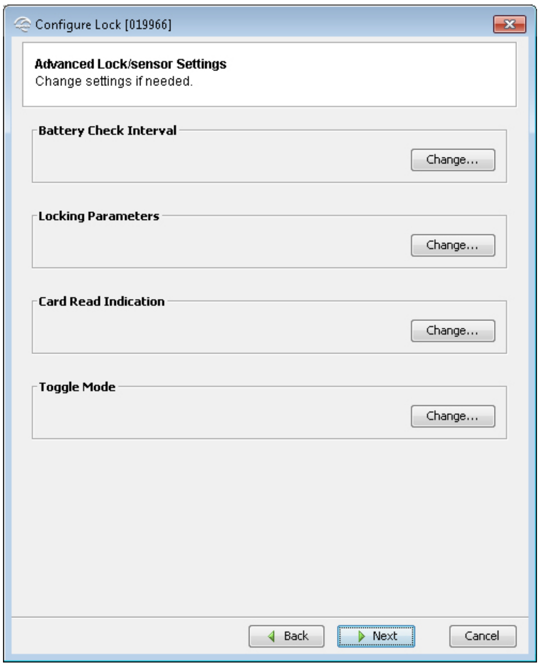
Device update result

Successfully updated radio channels.

To change radio channel in USB Radio Dongle, see section "*Offline Installation Settings" on page 8*.

Advanced Lock Settings

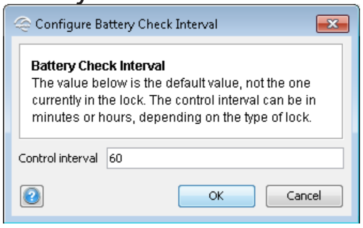
On this page you will be able to configure *Battery Check Interval*, *Status Report Interval*, *Locking Parameters*, *Card Read Indication* and *Toggle Mode*.



Configure Lock [019966]

Advanced Lock/sensor Settings
Change settings if needed.

Battery Check Interval



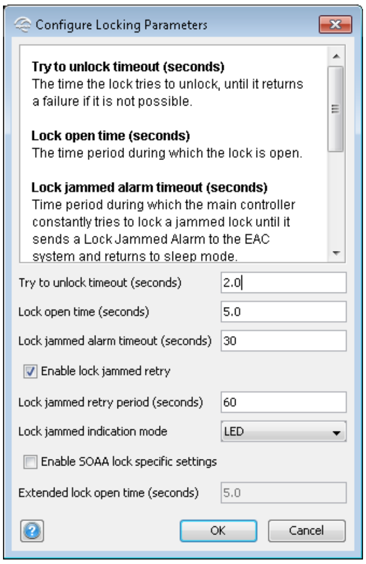
Configure Battery Check Interval

Battery Check Interval
The value below is the default value, not the one currently in the lock. The control interval can be in minutes or hours, depending on the type of lock.

Control interval: 60

When the battery power check detects low battery it is stored in the event log. The event log is written to a user credential and sent back to the EAC system through an offline updater. It may be necessary to adjust the time interval for this check depending on the type of battery used and the surrounding temperature, e.g. in cold surroundings the battery runs out faster. Default value is 60 (minutes).

Locking Parameters



Try to unlock timeout (seconds)
The time the lock tries to unlock, until it returns a failure if it is not possible.

Lock open time (seconds)
The time period during which the lock is open.

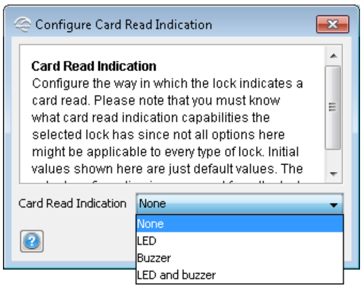
Lock jammed alarm timeout (seconds)
Time period during which the main controller constantly tries to lock a jammed lock until it sends a Lock Jammed Alarm to the EAC system and returns to sleep mode.

Try to unlock timeout (seconds): 2.0
Lock open time (seconds): 5.0
Lock jammed alarm timeout (seconds): 30
☑ Enable lock jammed retry
Lock jammed retry period (seconds): 60
Lock jammed indication mode: LED
☐ Enable SOAA lock specific settings
Extended lock open time (seconds): 5.0

Here you configure timing for different operations in the lock:

- **Try to unlock timeout (seconds):** How long the lock tries to unlock before it returns a failure.
- **Lock open time (seconds):** How long the lock will be open in seconds (default = 5 seconds).
- **Lock jammed alarm timeout (seconds):** How long time the lock tries to lock before an alarm flag is set and the lock return to idle state (default = 30 seconds).
- **Enable lock jammed retry:** This enables a periodic retry to lock according the settings under “Lock jammed retry period (seconds).
- **Lock jammed retry period (seconds):** How long the lock will wait before it retries to lock, in seconds (default = 60 seconds).
- **Lock jammed indication mode:** The way in which the lock indicates that it has been jammed. LED, Buzzer and LED and buzzer are the different indication modes.
- **Enable SOAA lock specific settings:** Click to enable SOAA specific settings.
- **Extended lock open time (seconds):** This setting enables an extended lock open time to be set for a SOAA lock. Default value 5.0 seconds. This setting is used to allow exceptions for certain user credentials to use the extended lock open time instead of the default value set by *Lock open time (seconds)* above.

Card Read Indication

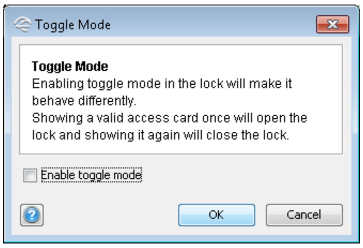


Card Read Indication
Configure the way in which the lock indicates a card read. Please note that you must know what card read indication capabilities the selected lock has since not all options here might be applicable to every type of lock. Initial values shown here are just default values. The

Card Read Indication: None

Different locks can have a different mechanism for audio-visual indication of successful credential reading. Here it is possible to disable credential read indication or to set it to LED. Some Aperio locks have support for other mechanisms such as buzzers.

Toggle mode



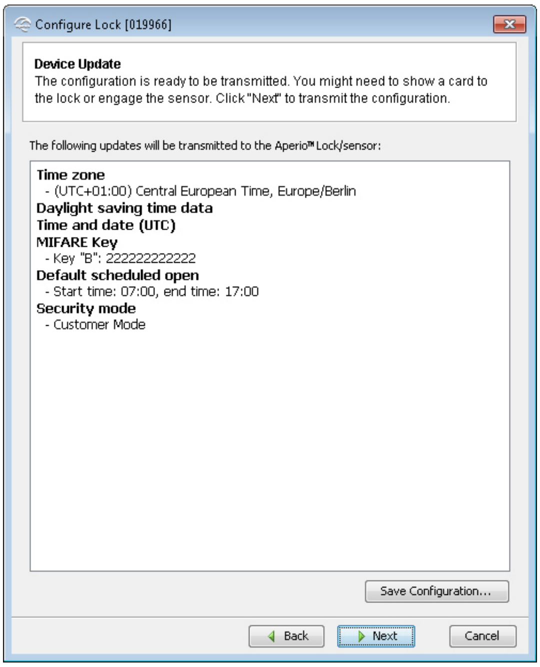
Toggle Mode
Enabling toggle mode in the lock will make it behave differently.
Showing a valid access card once will open the lock and showing it again will close the lock.

□ Enable toggle mode

If a lock is set in toggle mode then it will work exactly like a normal mechanical lock. Showing an access card will open the lock until the user shows the card again to close it. Toggle mode is by default turned off.

Device update page – Saving Configuration

Here a summary of configurations that will be transferred to the unit. The Device Update dialog box shows a summary of the configuration tasks that will be downloaded to the lock. The configuration may be used later to configure other devices with the same information, by clicking *Save configuration*:



Device Update
The configuration is ready to be transmitted. You might need to show a card to the lock or engage the sensor. Click "Next" to transmit the configuration.

The following updates will be transmitted to the Aperio™ Lock/sensor:

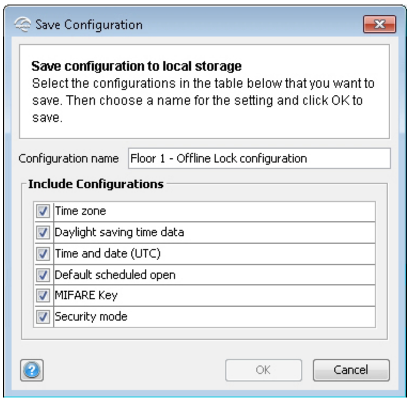
Time zone
- (UTC+01:00) Central European Time, Europe/Berlin

Daylight saving time data
Time and date (UTC)
MIFARE Key
- Key "B": 222222222222

Default scheduled open
- Start time: 07:00, end time: 17:00

Security mode
- Customer Mode

1) The *Save Configuration* dialog box shows a summary of the configuration tasks that have been collected during the different steps in the Configuration Wizard. Exclude configuration tasks by clicking the check boxes.



Save Configuration

Save configuration to local storage

Select the configurations in the table below that you want to save. Then choose a name for the setting and click OK to save.

Configuration name: Floor 1 - Offline Lock configuration

Include Configurations

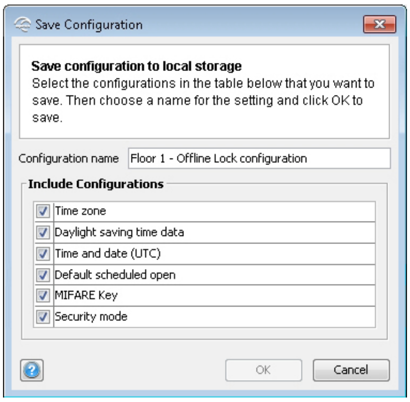
- ☑ Time zone
- ☑ Daylight saving time data
- ☑ Time and date (UTC)
- ☑ Default scheduled open
- ☑ MIFARE Key
- ☑ Security mode

2) Recommended tasks to save could be:
   a) RFID configuration
   b) Change security mode
   c) Device time update
   d) And optionally some advanced features like Battery Alarm, Status configuration and Locking parameters.

If you choose to save a configuration, keep in mind that some configuration settings should not be saved. Only save settings that are general for all locks in your installation.

Tip: Create a set of configurations for the most common settings in your system.

3) Enter a unique and suitable name for this configuration in the Configuration name field. Choose this name carefully, to make it clear what settings are changed in the lock/sensor or communication hub. You could, for instance, name it according to the different configuration tasks or, if applicable, use a name that reflects the specific door type.



Save Configuration

Save configuration to local storage

Select the configurations in the table below that you want to save. Then choose a name for the setting and click OK to save.

Configuration name: Floor 1 - Offline Lock configuration

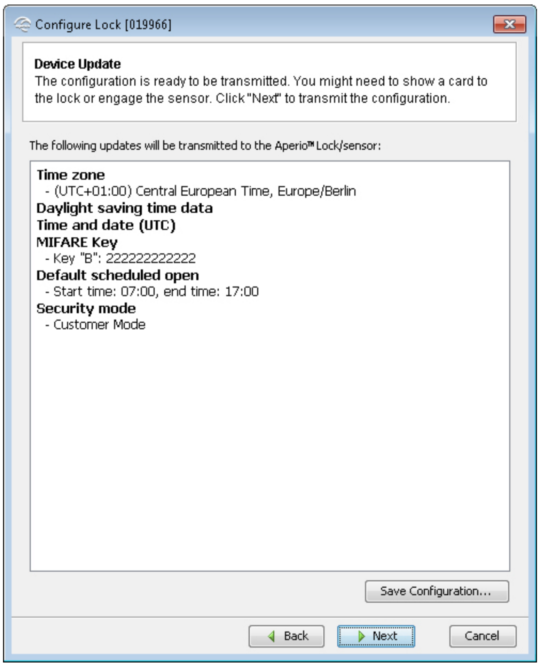
Include Configurations

- ☑ Time zone
- ☑ Daylight saving time data
- ☑ Time and date (UTC)
- ☑ Default scheduled open
- ☑ MIFARE Key
- ☑ Security mode

4) Click *OK*.

Result: The configuration is saved in the local storage, and you are back in the Configuration Wizard. Choosing *Cancel* on the Device Update page does not affect the locally stored configuration.

5) Click *Next* to download the configuration to the lock.



Device Update

The configuration is ready to be transmitted. You might need to show a card to the lock or engage the sensor. Click "Next" to transmit the configuration.

The following updates will be transmitted to the Aperio™ Lock/sensor:

Time zone
- (UTC+01:00) Central European Time, Europe/Berlin

Daylight saving time data

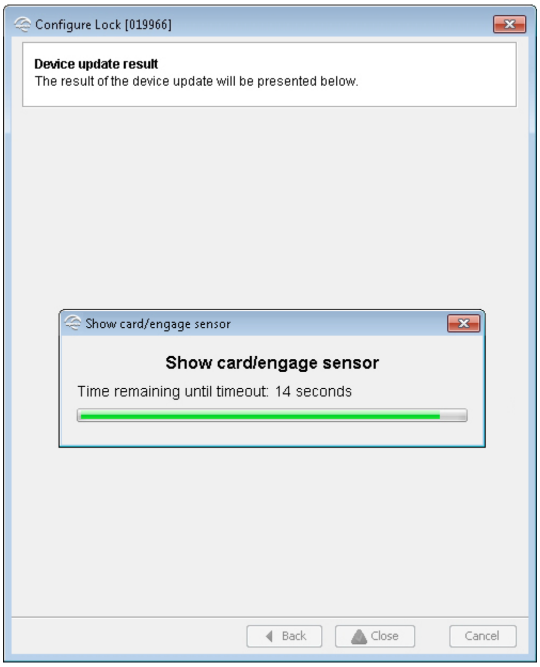
Time and date (UTC)

MIFARE Key
- Key "B": 222222222222

Default scheduled open
- Start time: 07:00, end time: 17:00

Security mode
- Customer Mode

6) Hold the radio card at the lock (or remove and reinsert battery).



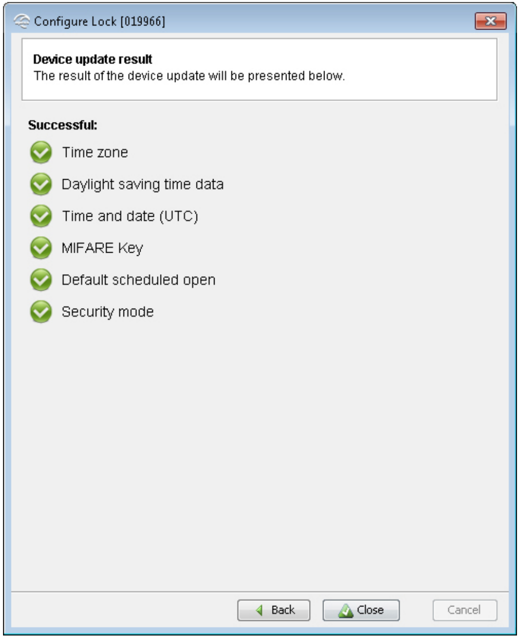
Device update result

The result of the device update will be presented below.

Show card/engage sensor

Time remaining until timeout: 14 seconds

7) Click *Close* to exit the wizard.



Configure Lock [019966]

Device update result

The result of the device update will be presented below.

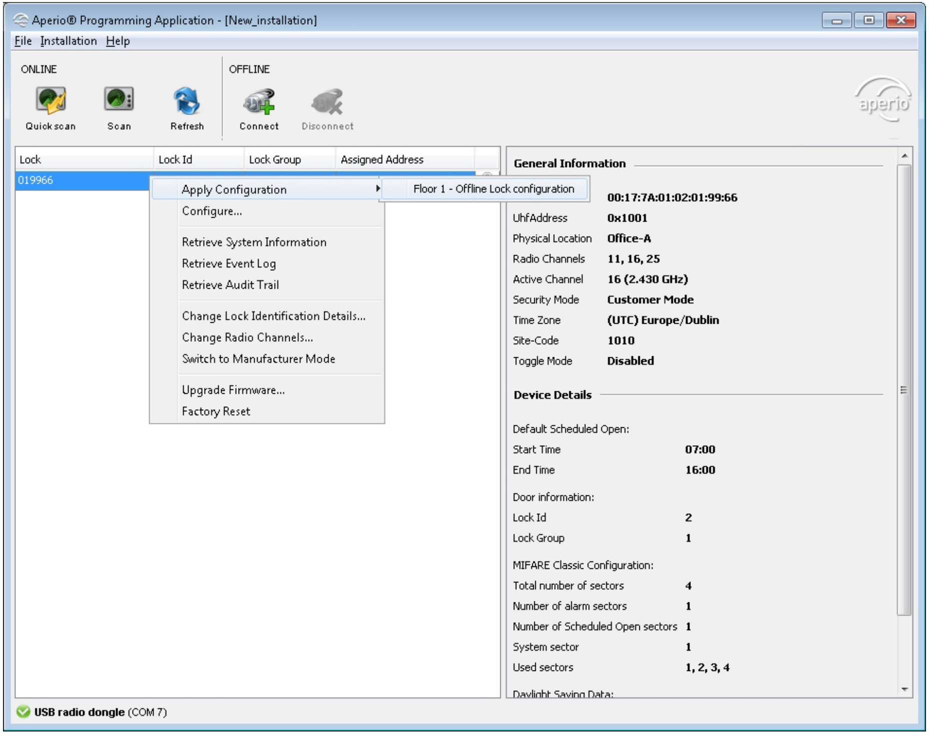
Successful:

- ✓ Time zone
- ✓ Daylight saving time data
- ✓ Time and date (UTC)
- ✓ MIFARE Key
- ✓ Default scheduled open
- ✓ Security mode

Applying a stored configuration to a lock

If you saved a configuration in the configuration wizard, you can apply it to numerous locks. Follow these steps to download a saved configuration to a lock:

1) Connect to another lock that you want to apply a saved configuration on. In the Installation view, right-click the new lock and select *Apply configuration* and choose an earlier stored configuration.



Aperio® Programming Application - [New_installation]

Lock	Lock Id	Lock Group	Assigned Address
019966			

General Information

	00:17:7A:01:02:01:99:66
UhfAddress	0x1001
Physical Location	Office-A
Radio Channels	11, 16, 25
Active Channel	16 (2.430 GHz)
Security Mode	Customer Mode
Time Zone	(UTC) Europe/Dublin
Site-Code	1010
Toggle Mode	Disabled

Device Details

Default Scheduled Open:

Start Time	07:00
End Time	16:00

Door information:

Lock Id	2
Lock Group	1

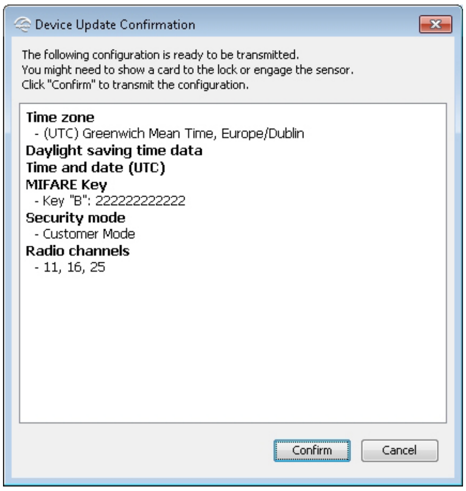
MIFARE Classic Configuration:

Total number of sectors	4
Number of alarm sectors	1
Number of Scheduled Open sectors	1
System sector	1
Used sectors	1, 2, 3, 4

Daylight Saving Data:

✓ USB radio dongle (COM 7)

2) Click *Confirm* to start the transfer.



Device Update Confirmation

The following configuration is ready to be transmitted.
You might need to show a card to the lock or engage the sensor.
Click "Confirm" to transmit the configuration.

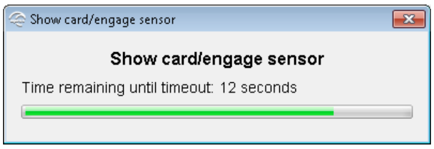
Time zone
- (UTC) Greenwich Mean Time, Europe/Dublin

Daylight saving time data
Time and date (UTC)
MIFARE Key
- Key "B": 222222222222

Security mode
- Customer Mode

Radio channels
- 11, 16, 25

3) Hold the radio activation card at the lock (or remove and reinsert the battery) to download the configuration.

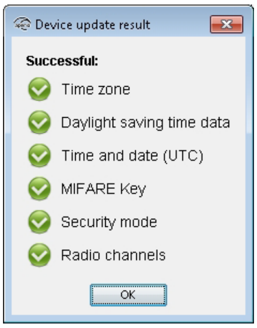


Show card/engage sensor

Show card/engage sensor

Time remaining until timeout: 12 seconds

4) After download the result is shown. The settings that could not be downloaded to the specific hardware are ignored. Click *OK* to finish.



Device update result

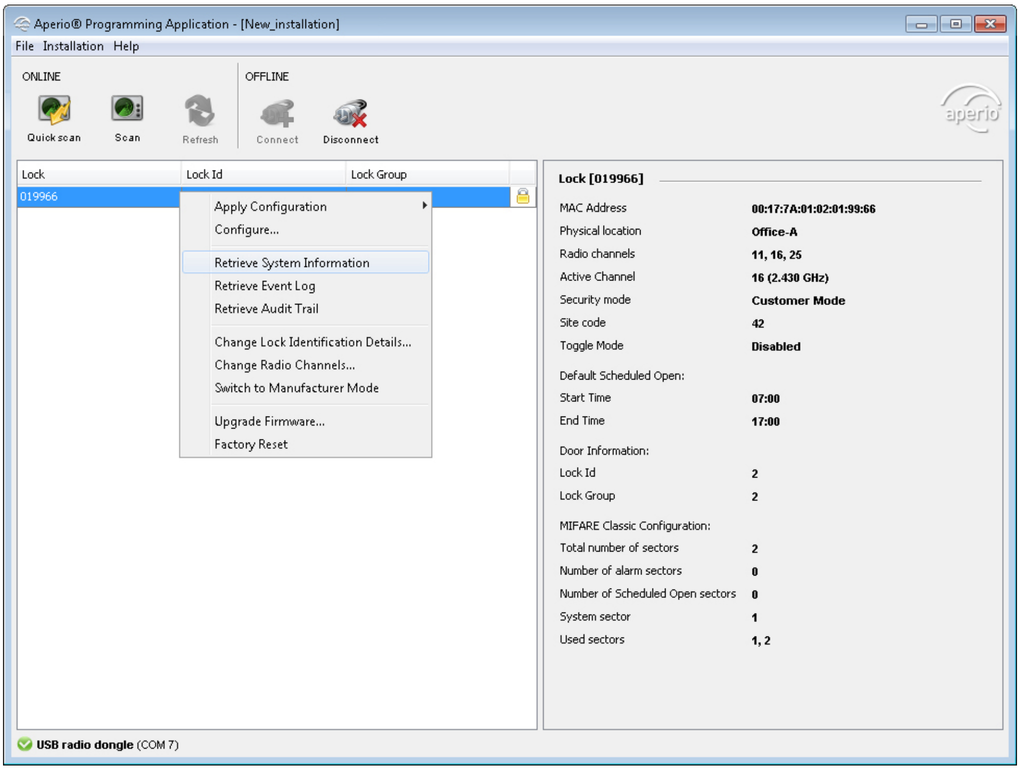
Successful:

✓ Time zone
✓ Daylight saving time data
✓ Time and date (UTC)
✓ MIFARE Key
✓ Security mode
✓ Radio channels

5) Repeat all the steps from the beginning of this section for every lock you want to configure with a saved configuration.

Retrieve system information

1) Right-click and select *Retrieve system information* to access the unit.

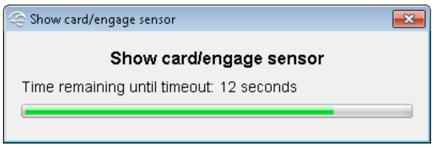


Lock [019966]

MAC Address	00:17:7A:01:02:01:99:66
Physical location	Office-A
Radio channels	11, 16, 25
Active Channel	16 (2.430 GHz)
Security mode	Customer Mode
Site code	42
Toggle Mode	Disabled
Default Scheduled Open:	
Start Time	07:00
End Time	17:00
Door Information:	
Lock Id	2
Lock Group	2
MIFARE Classic Configuration:	
Total number of sectors	2
Number of alarm sectors	0
Number of Scheduled Open sectors	0
System sector	1
Used sectors	1, 2

USB radio dongle (COM 7)

2) Hold the radio activation card at the lock (or remove and reinsert the battery) to access the unit.

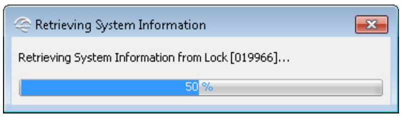


Show card/engage sensor

Show card/engage sensor

Time remaining until timeout: 12 seconds

Result: The Programming Application connects to the unit.

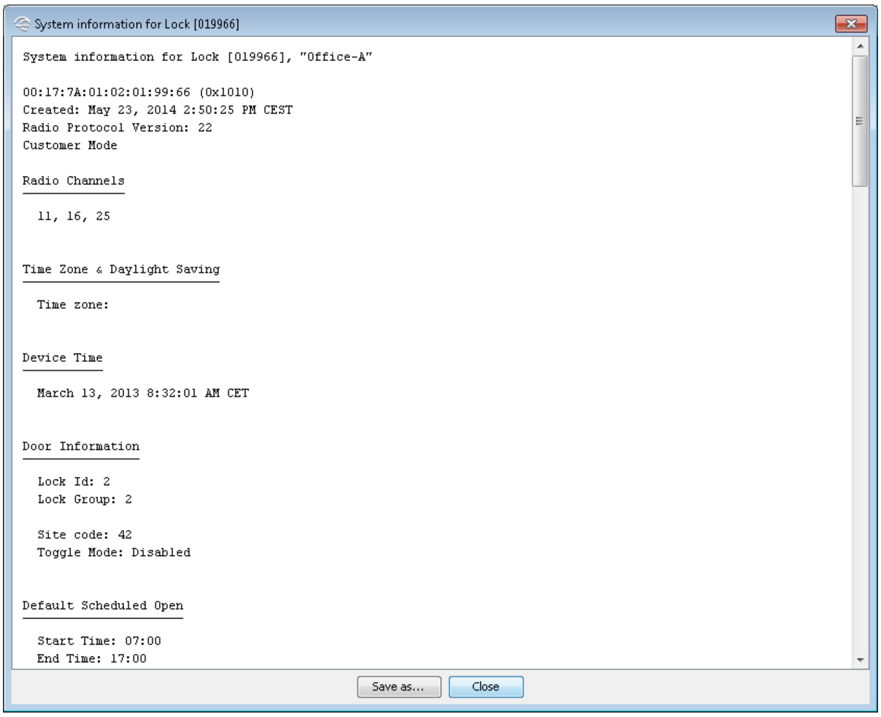


Retrieving System Information

Retrieving System Information from Lock [019966]...

50 %

3) Click *Save as...* to save the system information to a local storage or click *Close* to exit.

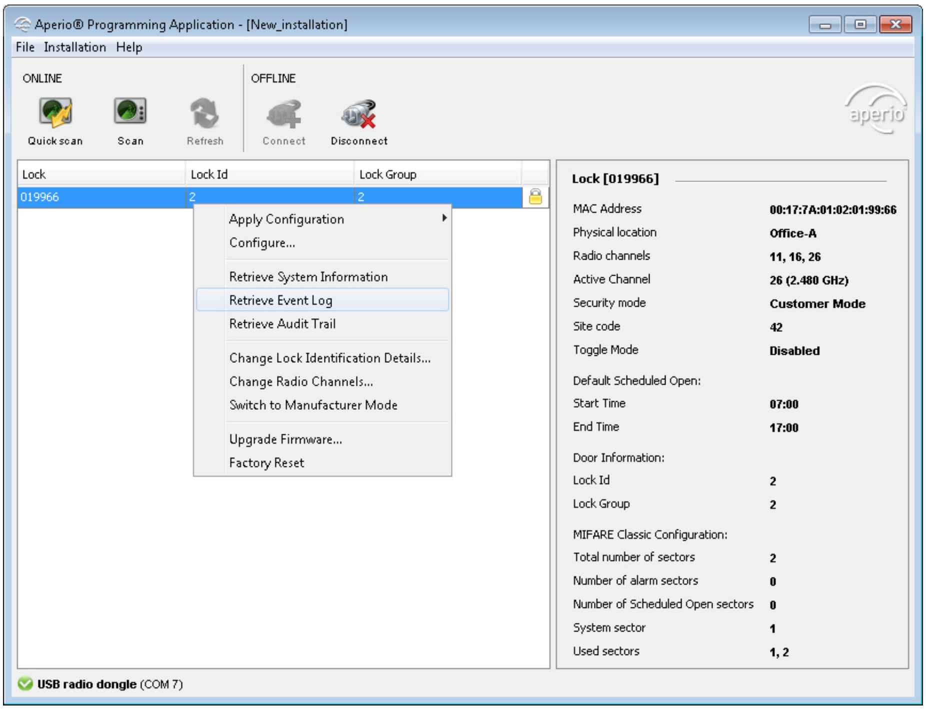


```
System information for Lock [019966], "Office-A"

00:17:7A:01:02:01:99:66 (0x1010)
Created: May 23, 2014 2:50:25 PM CEST
Radio Protocol Version: 22
Customer Mode

Radio Channels

  11, 16, 25


Time Zone & Daylight Saving

  Time zone:


Device Time

  March 13, 2013 8:32:01 AM CET


Door Information

  Lock Id: 2
  Lock Group: 2

  Site code: 42
  Toggle Mode: Disabled


Default Scheduled Open

  Start Time: 07:00
  End Time: 17:00
```

Retrieve Event Log

This function displays the event log for a particular lock (not available for sensor), where you can find all system events performed on the lock.

1) Right-click and select *Lock/sensor-Retrive Event Log*

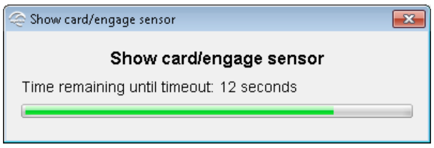


Lock [019966]

MAC Address	00:17:7A:01:02:01:99:66
Physical location	Office-A
Radio channels	11, 16, 26
Active Channel	26 (2.480 GHz)
Security mode	Customer Mode
Site code	42
Toggle Mode	Disabled
Default Scheduled Open:	
Start Time	07:00
End Time	17:00
Door Information:	
Lock Id	2
Lock Group	2
MIFARE Classic Configuration:	
Total number of sectors	2
Number of alarm sectors	0
Number of Scheduled Open sectors	0
System sector	1
Used sectors	1, 2

USB radio dongle (COM 7)

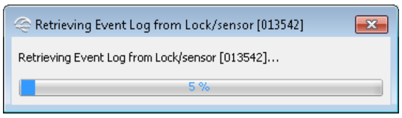
2) Hold the radio activation card at the lock (or remove and reinsert the battery).



Show card/engage sensor

Time remaining until timeout: 12 seconds

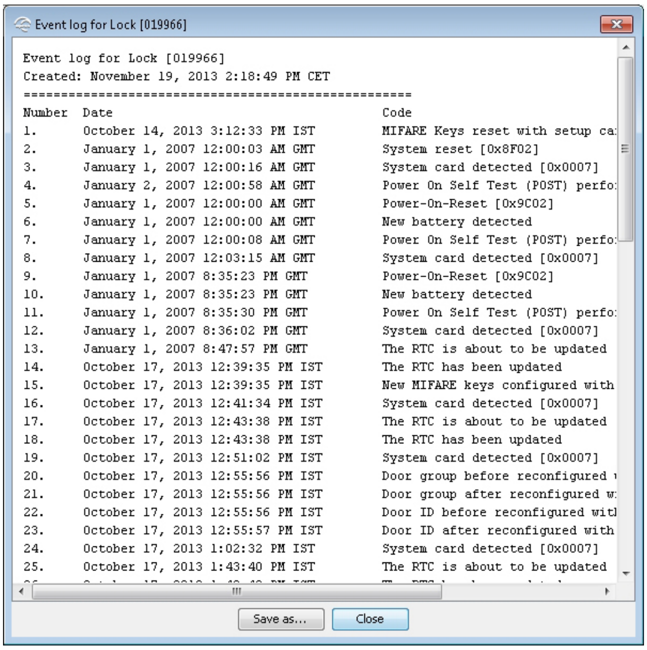
3) **Result:** Successful reading initiates the download of the event log.



Retrieving Event Log from Lock/sensor [013542]...

5 %

4) In the event log window, click Save As to save the information to a *.txt-file or click Close to exit without saving.



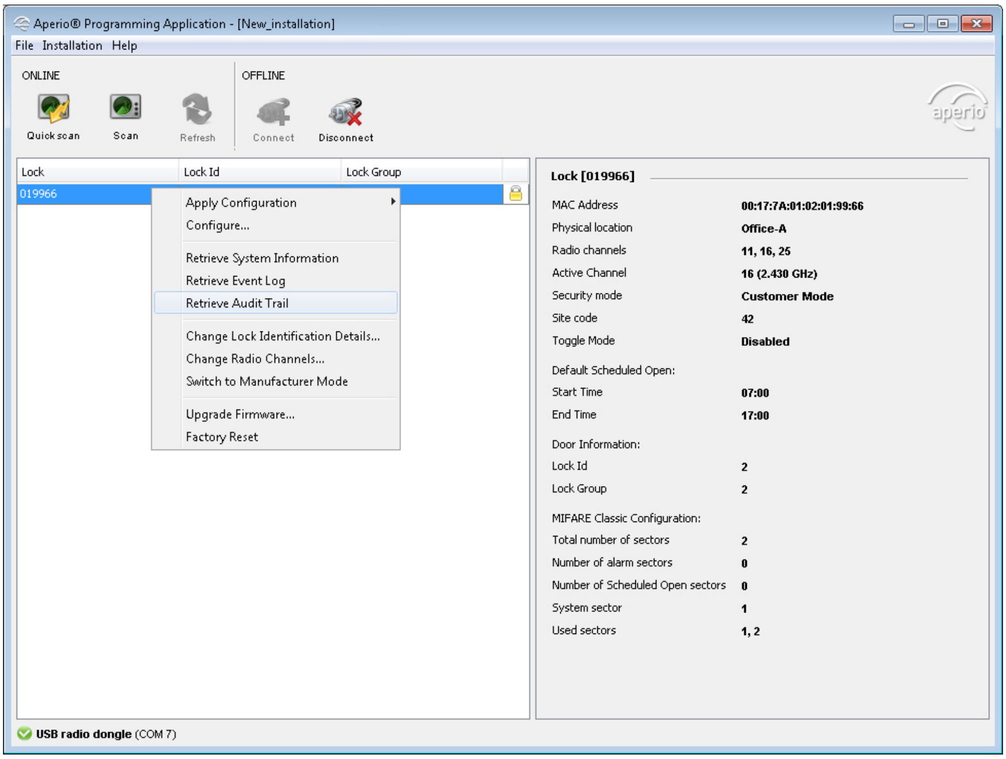
```
Event log for Lock [019966]
Created: November 19, 2013 2:18:49 PM CET
====================================================
Number  Date                                    Code
1.      October 14, 2013 3:12:33 PM IST         MIFARE Keys reset with setup ca
2.      January 1, 2007 12:00:03 AM GMT         System reset [0x8F02]
3.      January 1, 2007 12:00:16 AM GMT         System card detected [0x0007]
4.      January 2, 2007 12:00:58 AM GMT         Power On Self Test (POST) perfo
5.      January 1, 2007 12:00:00 AM GMT         Power-On-Reset [0x9C02]
6.      January 1, 2007 12:00:00 AM GMT         New battery detected
7.      January 1, 2007 12:00:08 AM GMT         Power On Self Test (POST) perfo
8.      January 1, 2007 12:03:15 AM GMT         System card detected [0x0007]
9.      January 1, 2007 8:35:23 PM GMT          Power-On-Reset [0x9C02]
10.     January 1, 2007 8:35:23 PM GMT          New battery detected
11.     January 1, 2007 8:35:30 PM GMT          Power On Self Test (POST) perfo
12.     January 1, 2007 8:36:02 PM GMT          System card detected [0x0007]
13.     January 1, 2007 8:47:57 PM GMT          The RTC is about to be updated
14.     October 17, 2013 12:39:35 PM IST        The RTC has been updated
15.     October 17, 2013 12:39:35 PM IST        New MIFARE keys configured with
16.     October 17, 2013 12:41:34 PM IST        System card detected [0x0007]
17.     October 17, 2013 12:43:38 PM IST        The RTC is about to be updated
18.     October 17, 2013 12:43:38 PM IST        The RTC has been updated
19.     October 17, 2013 12:51:02 PM IST        System card detected [0x0007]
20.     October 17, 2013 12:55:56 PM IST        Door group before reconfigured
21.     October 17, 2013 12:55:56 PM IST        Door group after reconfigured w
22.     October 17, 2013 12:55:56 PM IST        Door ID before reconfigured wit
23.     October 17, 2013 12:55:57 PM IST        Door ID after reconfigured with
24.     October 17, 2013 1:02:32 PM IST         System card detected [0x0007]
25.     October 17, 2013 1:43:40 PM IST         The RTC is about to be updated
```

This window contains a listing of the recent system events along with the date when it was observed. (If the number of events exceeds 200, older events are overwritten.)

Retrieve Audit Trail

This function displays a complete list of all access attempts for a particular lock.

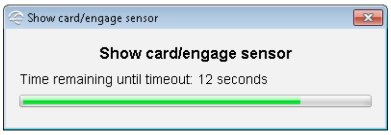
1) Right-click and select *Retrieve Audit Trail*.



Lock [019966]

MAC Address	00:17:7A:01:02:01:99:66
Physical location	Office-A
Radio channels	11, 16, 25
Active Channel	16 (2.430 GHz)
Security mode	Customer Mode
Site code	42
Toggle Mode	Disabled
Default Scheduled Open:	
Start Time	07:00
End Time	17:00
Door Information:	
Lock Id	2
Lock Group	2
MIFARE Classic Configuration:	
Total number of sectors	2
Number of alarm sectors	0
Number of Scheduled Open sectors	0
System sector	1
Used sectors	1, 2

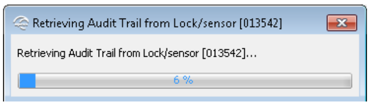
2) Hold the radio activation card at the lock (or remove and reinsert the battery).



Show card/engage sensor

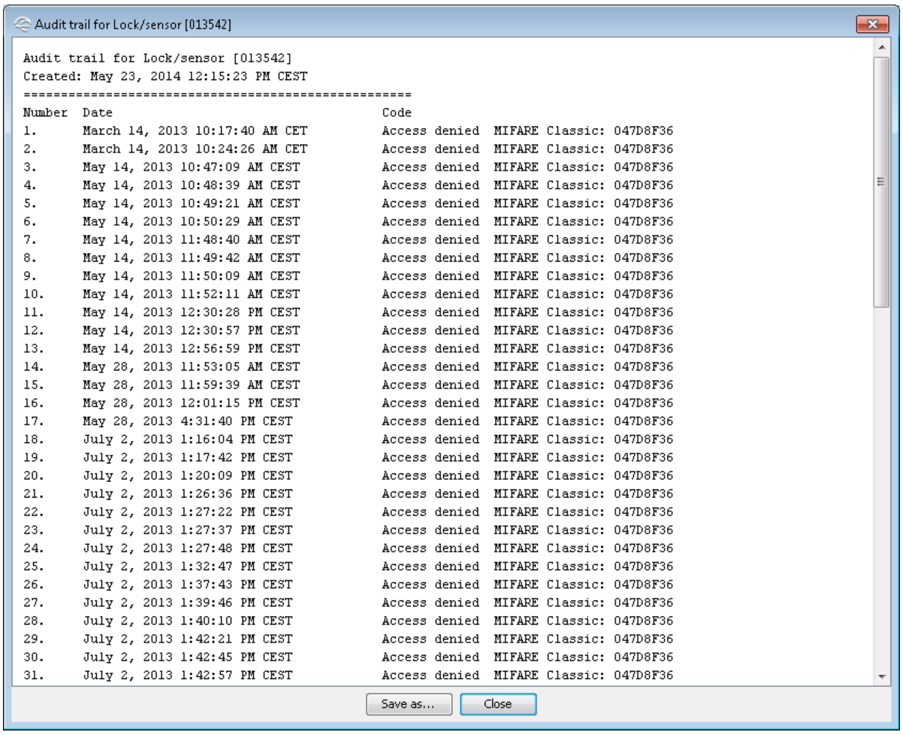
Time remaining until timeout: 12 seconds

Result: Successful reading initiates the download of the audit trail.



Retrieving Audit Trail from Lock/sensor [013542]...

3) In the audit trail window, click *Save As* to save the information to a *.txt-file or click Close to exit without saving.



```
Audit trail for Lock/sensor [013542]
Created: May 23, 2014 12:15:23 PM CEST
====================================================
Number  Date                                    Code
1.      March 14, 2013 10:17:40 AM CET          Access denied  MIFARE Classic: 047D8F36
2.      March 14, 2013 10:24:26 AM CET          Access denied  MIFARE Classic: 047D8F36
3.      May 14, 2013 10:47:09 AM CEST           Access denied  MIFARE Classic: 047D8F36
4.      May 14, 2013 10:48:39 AM CEST           Access denied  MIFARE Classic: 047D8F36
5.      May 14, 2013 10:49:21 AM CEST           Access denied  MIFARE Classic: 047D8F36
6.      May 14, 2013 10:50:29 AM CEST           Access denied  MIFARE Classic: 047D8F36
7.      May 14, 2013 11:48:40 AM CEST           Access denied  MIFARE Classic: 047D8F36
8.      May 14, 2013 11:49:42 AM CEST           Access denied  MIFARE Classic: 047D8F36
9.      May 14, 2013 11:50:09 AM CEST           Access denied  MIFARE Classic: 047D8F36
10.     May 14, 2013 11:52:11 AM CEST           Access denied  MIFARE Classic: 047D8F36
11.     May 14, 2013 12:30:28 PM CEST           Access denied  MIFARE Classic: 047D8F36
12.     May 14, 2013 12:30:57 PM CEST           Access denied  MIFARE Classic: 047D8F36
13.     May 14, 2013 12:56:59 PM CEST           Access denied  MIFARE Classic: 047D8F36
14.     May 28, 2013 11:53:05 AM CEST           Access denied  MIFARE Classic: 047D8F36
15.     May 28, 2013 11:59:39 AM CEST           Access denied  MIFARE Classic: 047D8F36
16.     May 28, 2013 12:01:15 PM CEST           Access denied  MIFARE Classic: 047D8F36
17.     May 28, 2013 4:31:40 PM CEST            Access denied  MIFARE Classic: 047D8F36
18.     July 2, 2013 1:16:04 PM CEST            Access denied  MIFARE Classic: 047D8F36
19.     July 2, 2013 1:17:42 PM CEST            Access denied  MIFARE Classic: 047D8F36
20.     July 2, 2013 1:20:09 PM CEST            Access denied  MIFARE Classic: 047D8F36
21.     July 2, 2013 1:26:36 PM CEST            Access denied  MIFARE Classic: 047D8F36
22.     July 2, 2013 1:27:22 PM CEST            Access denied  MIFARE Classic: 047D8F36
23.     July 2, 2013 1:27:37 PM CEST            Access denied  MIFARE Classic: 047D8F36
24.     July 2, 2013 1:27:48 PM CEST            Access denied  MIFARE Classic: 047D8F36
25.     July 2, 2013 1:32:47 PM CEST            Access denied  MIFARE Classic: 047D8F36
26.     July 2, 2013 1:37:43 PM CEST            Access denied  MIFARE Classic: 047D8F36
27.     July 2, 2013 1:39:46 PM CEST            Access denied  MIFARE Classic: 047D8F36
28.     July 2, 2013 1:40:10 PM CEST            Access denied  MIFARE Classic: 047D8F36
29.     July 2, 2013 1:42:21 PM CEST            Access denied  MIFARE Classic: 047D8F36
30.     July 2, 2013 1:42:45 PM CEST            Access denied  MIFARE Classic: 047D8F36
31.     July 2, 2013 1:42:57 PM CEST            Access denied  MIFARE Classic: 047D8F36
```

This window contains a listing of the total number of access attempts showing date, access decision and credential type.

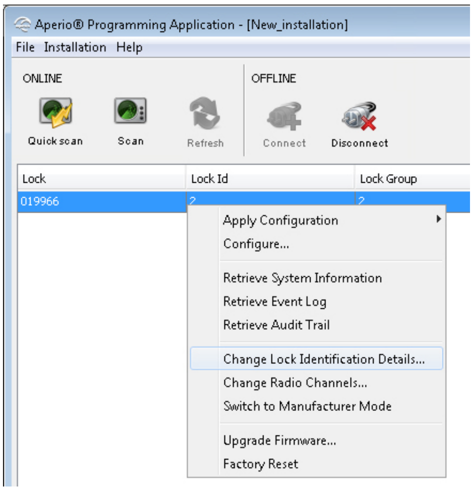
Change lock identification details

This menu option will allow the user to change Lock ID, Group & Physical location. Lock ID is used as an identifier for each lock. Lock Group is used to cluster several locks for example in order to create access areas, where all the locks in one group will use the same access settings. Physical location is just a logical name for the lock.

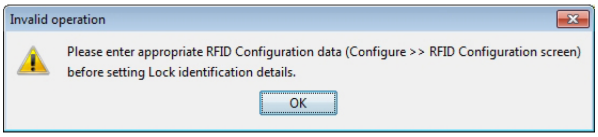
If a SOAA lock is used, it can belong to multiple lock groups (8 max) or no lock group at all.

The maximum number of lock groups is decided by the sector configuration done in the configure lock function, see section *RFID configuration*.

1) Select the lock, right-click and select *Change Lock Identification Details...*



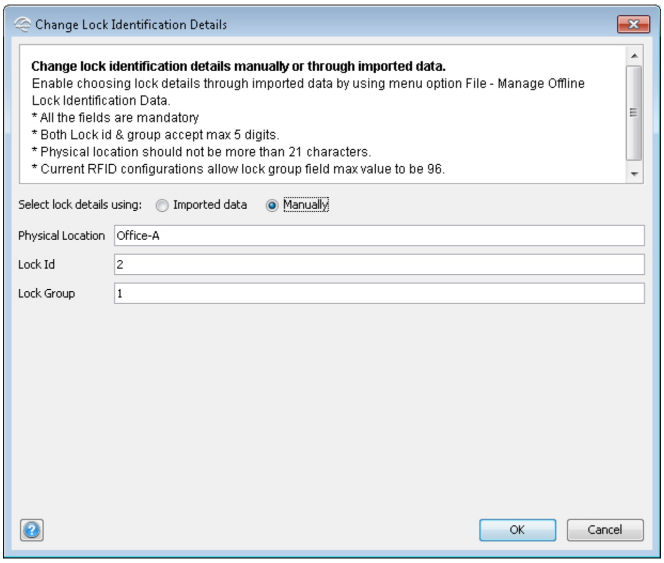
2) User should always (not necessary for SOAA) set RFID configurations (see section RFID configuration) before changing/adding lock identification details. However if a user tries to set lock identification details before setting RFID configurations then following screen will be shown to the user.


Invalid operation

Please enter appropriate RFID Configuration data (Configure >> RFID Configuration screen) before setting Lock identification details.

3) Set lock identification details either *Manually* or through *Imported data* by selecting one of the radio buttons.

a) **Manually:** Enter *Physical Location* (max 20 alpha numeric characters), *Lock Id* (max 5 numeric characters), *Lock Group* (max 5 numeric characters & max value decided by RFID configurations).



Change Lock Identification Details

Change lock identification details manually or through imported data.
Enable choosing lock details through imported data by using menu option File - Manage Offline Lock Identification Data.
* All the fields are mandatory
* Both Lock id & group accept max 5 digits.
* Physical location should not be more than 21 characters.
* Current RFID configurations allow lock group field max value to be 96.

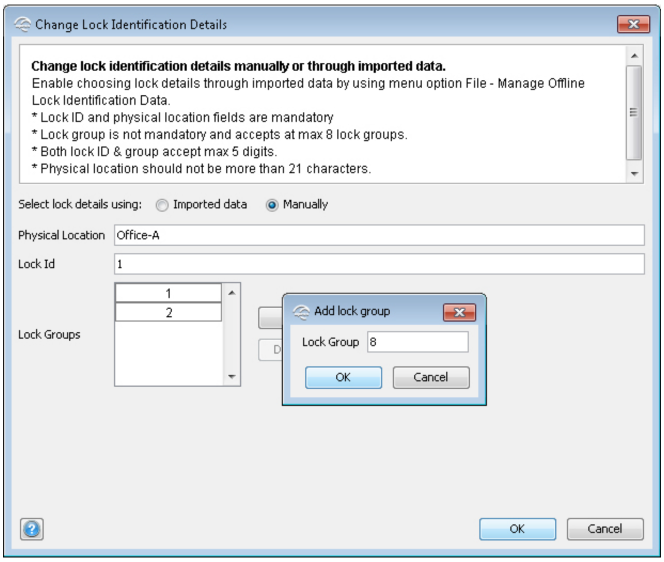
Select lock details using: ○ Imported data ● Manually

Physical Location: Office-A

Lock Id: 2

Lock Group: 1

Manually - connected to a SOAA lock: Enter value for *Lock Groups* (max 5 numeric characters, 2 bytes (0-65535)). Up to 8 lock groups can be added. No lock group belonging is also allowed.



Change Lock Identification Details

Change lock identification details manually or through imported data.
Enable choosing lock details through imported data by using menu option File - Manage Offline Lock Identification Data.
* Lock ID and physical location fields are mandatory
* Lock group is not mandatory and accepts at max 8 lock groups.
* Both lock ID & group accept max 5 digits.
* Physical location should not be more than 21 characters.

Select lock details using: ○ Imported data ● Manually

Physical Location: Office-A

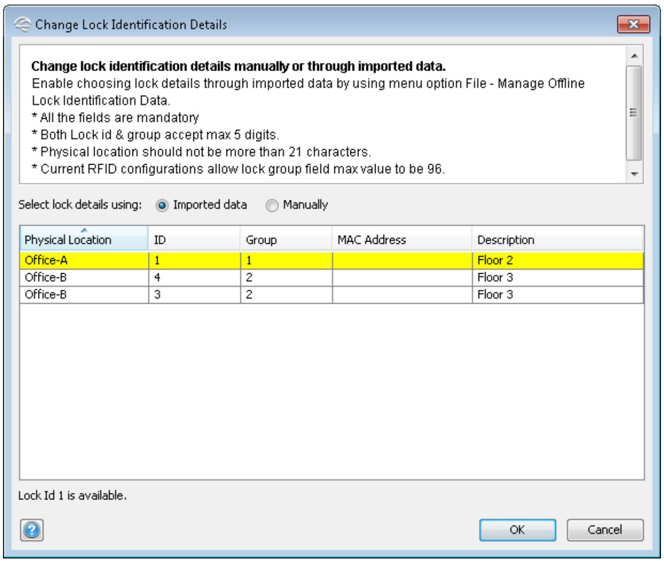
Lock Id: 1

Lock Groups: 1, 2

Add lock group

Lock Group: 8

b) **Imported data:** This option can be used if lock identification details have been imported using the function *Installation - Offline - Manage Offline Lock Identification Data*, see section "*Manage Offline Lock Identification Data" on page 104*. After import, lock identification details will automatically be displayed here. Select lock identification details in the list by clicking the desired row.



Change Lock Identification Details

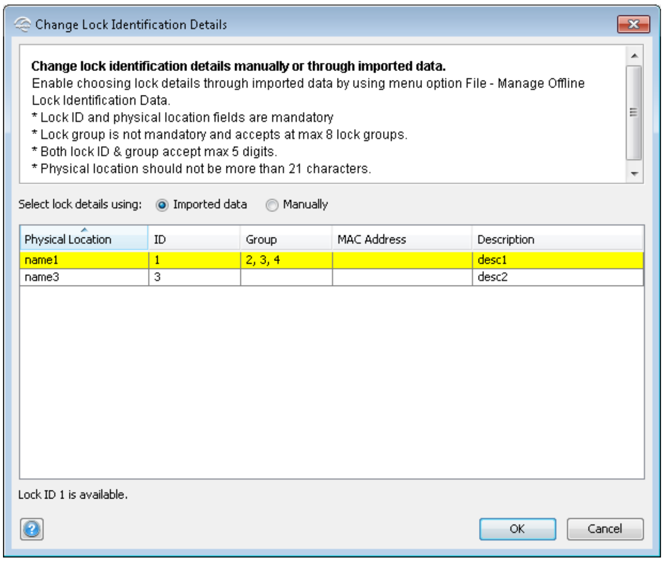
Change lock identification details manually or through imported data.
Enable choosing lock details through imported data by using menu option File - Manage Offline Lock Identification Data.
* All the fields are mandatory
* Both Lock id & group accept max 5 digits.
* Physical location should not be more than 21 characters.
* Current RFID configurations allow lock group field max value to be 96.

Select lock details using: ● Imported data ○ Manually

Physical Location	ID	Group	MAC Address	Description
Office-A	1	1		Floor 2
Office-B	4	2		Floor 3
Office-B	3	2		Floor 3

Lock Id 1 is available.

Imported data - connected to a SOAA lock: Select lock identification details in the list by clicking the desired row.



Change Lock Identification Details

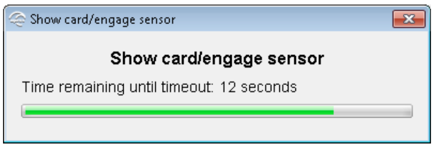
Change lock identification details manually or through imported data.
Enable choosing lock details through imported data by using menu option File - Manage Offline Lock Identification Data.
* Lock ID and physical location fields are mandatory
* Lock group is not mandatory and accepts at max 8 lock groups.
* Both lock ID & group accept max 5 digits.
* Physical location should not be more than 21 characters.

Select lock details using: ● Imported data ○ Manually

Physical Location	ID	Group	MAC Address	Description
name1	1	2, 3, 4		desc1
name3	3			desc2

Lock ID 1 is available.

4) Hold the radio card at the lock (or remove and reinsert battery) to download the Physical location data.



Show card/engage sensor

Show card/engage sensor

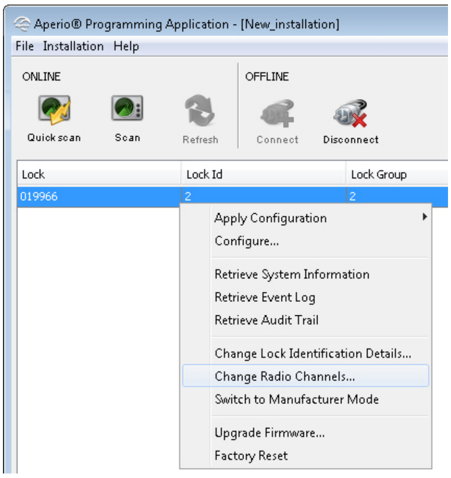
Time remaining until timeout: 12 seconds

Change Radio Channels

Changing the radio channel can be necessary if you experience interference between lock and USB Radio dongle.

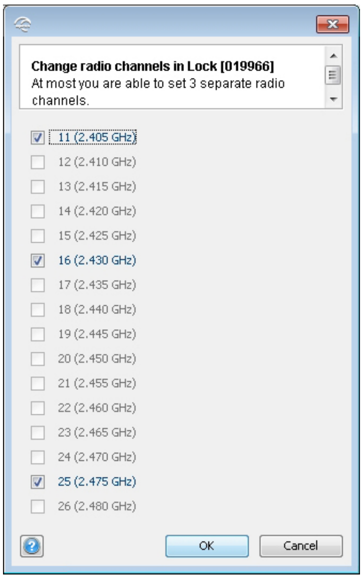
To use this function, you must have the *Show advanced settings* check box selected in *Preferences*, see section *"Preferences" on page* 9. Follow these steps to change the radio channel for the lock.

1) Select the lock in the scan result table. Right-click and select *Change Radio Channels...*



Lock	Lock Id	Lock Group
019966	2	2

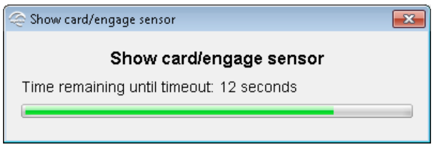
2) Uncheck any of the three currently used channels to be able to select other radio channels. Click *OK*.



Change radio channels in Lock [019966]
At most you are able to set 3 separate radio channels.

☑ 11 (2.405 GHz)
□ 12 (2.410 GHz)
□ 13 (2.415 GHz)
□ 14 (2.420 GHz)
□ 15 (2.425 GHz)
☑ 16 (2.430 GHz)
□ 17 (2.435 GHz)
□ 18 (2.440 GHz)
□ 19 (2.445 GHz)
□ 20 (2.450 GHz)
□ 21 (2.455 GHz)
□ 22 (2.460 GHz)
□ 23 (2.465 GHz)
□ 24 (2.470 GHz)
☑ 25 (2.475 GHz)
□ 26 (2.480 GHz)

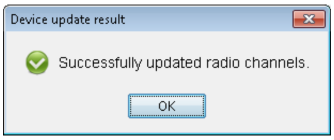
3) Hold the radio activation card at the lock (or remove and reinsert the battery) to perform the update.



Show card/engage sensor

Time remaining until timeout: 12 seconds

Result: A progress bar shows that the update is being performed. The Device update result dialog box shows the result of the update when it has been performed.



Device update result

Successfully updated radio channels.

To change radio channel in USB Radio Dongle, see section "*Offline Installation Settings" on page 8*.

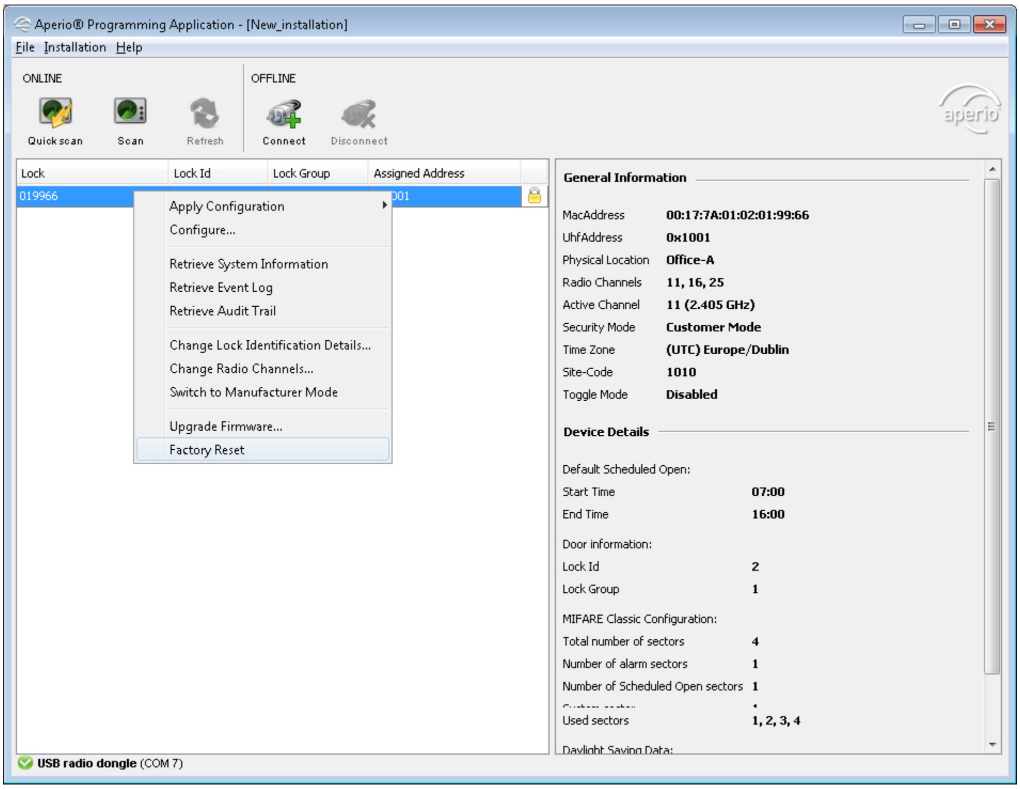
Change the Security Mode

This procedure is equal as for Aperio Online. *See section "Change the Security Mode" on page 58.*

Factory reset

When a factory reset is performed, lock id, lock group, site code, sector information, logs and the RFID Key(s) are erased from the lock. To reconnect and configure a lock that have been reset, you need to remove and reinstall the battery to activate the UHF transceiver in the lock.

1) Select lock, right-click and select *Factory reset*.



Aperio® Programming Application - [New_installation]

General Information

MacAddress **00:17:7A:01:02:01:99:66**
UhfAddress **0x1001**
Physical Location **Office-A**
Radio Channels **11, 16, 25**
Active Channel **11 (2.405 GHz)**
Security Mode **Customer Mode**
Time Zone **(UTC) Europe/Dublin**
Site-Code **1010**
Toggle Mode **Disabled**

Device Details

Default Scheduled Open:
Start Time **07:00**
End Time **16:00**

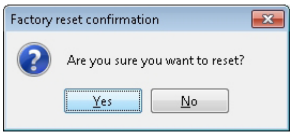
Door information:
Lock Id **2**
Lock Group **1**

MIFARE Classic Configuration:
Total number of sectors **4**
Number of alarm sectors **1**
Number of Scheduled Open sectors **1**
Used sectors **1, 2, 3, 4**

Daylight Saving Data:

USB radio dongle (COM 7)

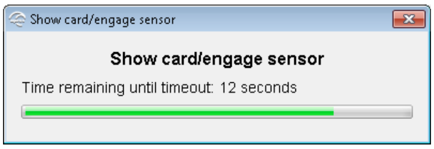
2) Confirm the reset by clicking *Yes*.



Factory reset confirmation

Are you sure you want to reset?

3) Hold the radio activation card at the lock (or remove and reinsert the battery) to download the change.



Show card/engage sensor

Show card/engage sensor

Time remaining until timeout: 12 seconds

Result: The lock is reset and disappears from the installation view.

Reconfiguration of lock after factory reset

To reconfigure a lock that has been reset without use of a factory default radio activation card:

1) Dismantle the lock cover and remove the battery from the lock.

2) Reinstall the same battery.
Result: The lock performs a power on self test, one red and one green flash. After that the UHF transceiver is activated - yellow blinking during 20 s.

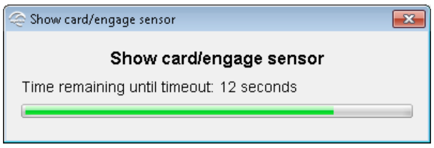
3) When the lock starts blinking yellow, click *Connect* in the menu bar.

4) When the lock is visible in the installation view, select the lock, right-click and select *Configure*. (Or *Apply configuration [your configuration]* if it contains your MIFARE Classic/DESFire Key configuration.)

5) On the first page in the Wizard, in the Change RFID Key configuration section, click *Change* and add the MIFARE Classic/DESFire configuration (see section *"RFID configuration (Lock/sensor)" on page 18*), depending upon the type of lock that you have.

6) Repeatedly, click *Next* on the rest of the pages in the Wizard until the download starts.

7) Hold the radio activation card at the lock (or remove and reinsert the battery) to download the change.

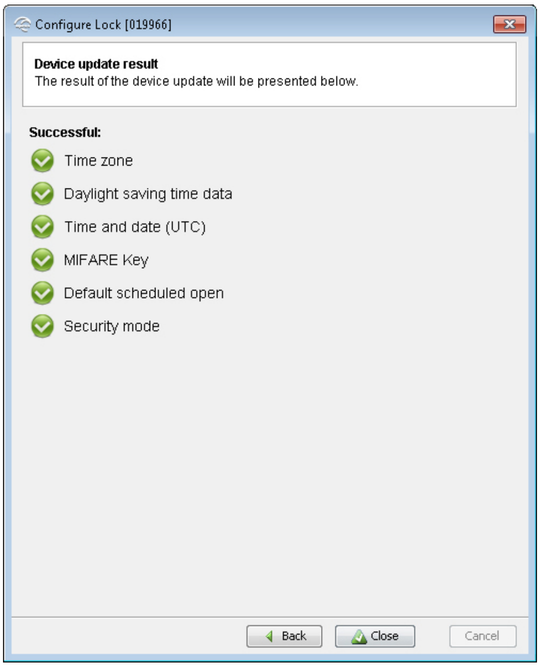


Show card/engage sensor

Show card/engage sensor

Time remaining until timeout: 12 seconds

After this the lock is updated with the MIFARE Classic/DESFire key that applies for your system.



Configure Lock [019966]

Device update result
The result of the device update will be presented below.

Successful:

- ✓ Time zone
- ✓ Daylight saving time data
- ✓ Time and date (UTC)
- ✓ MIFARE Key
- ✓ Default scheduled open
- ✓ Security mode

Reconfigure the lock with appropriate settings. Lock identification details must also always be reconfigured after a factory reset, see section "*Change lock identification details" on page 98*.

Importing and exporting configurations

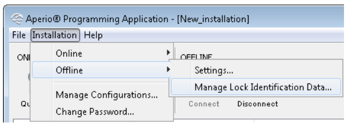
This procedure is equal as for Aperio Online, see section "*Managing configurations" on page 65*.

Manage Offline Lock Identification Data

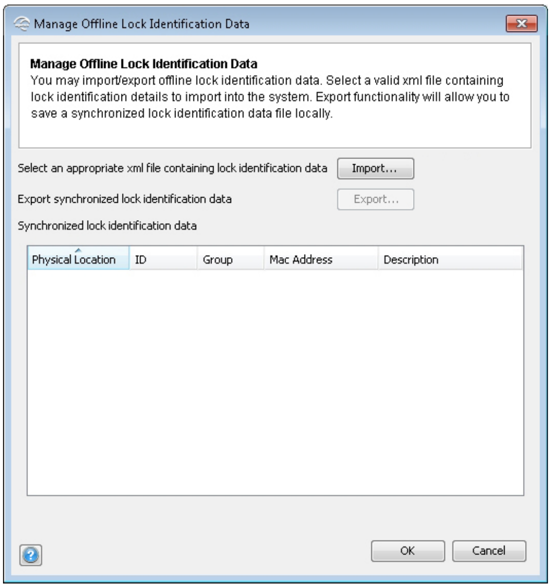
This function allows import of lock identification data from an EAC system in the form of an XML. After installation, the lock identification data (changes made during installation on the site) is exported back for use in the EAC system.

Importing lock identification data

1) Select *Installation - Offline - Manage Offline Lock Identification Data*.



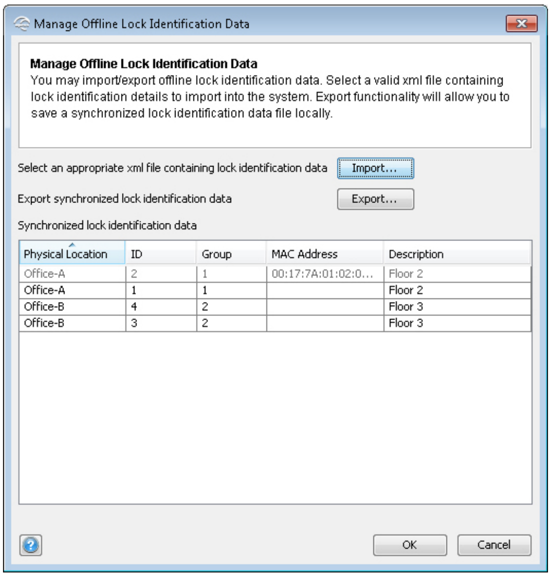
2) Click the *Import...* button to open the XML-file created by the EAC or manually (according to specified XML structure, see section *"Lock Identification Data XML format" on page 106*).



Manage Offline Lock Identification Data
Select an appropriate xml file containing lock identification data
Import...
Export synchronized lock identification data
Export...
Synchronized lock identification data
Physical Location
ID
Group
Mac Address
Description
OK
Cancel

Manage Offline Lock Identification Data
You may import/export offline lock identification data. Select a valid xml file containing lock identification details to import into the system. Export functionality will allow you to save a synchronized lock identification data file locally.

Result: The lock identification data is displayed. Exit the dialog by clicking *OK*.



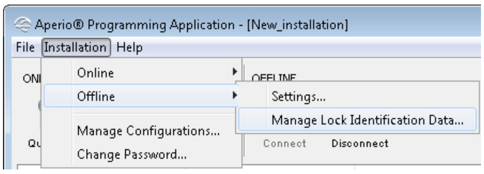
Manage Offline Lock Identification Data
Select an appropriate xml file containing lock identification data
Import...
Export synchronized lock identification data
Export...
Synchronized lock identification data
OK
Cancel

Manage Offline Lock Identification Data
You may import/export offline lock identification data. Select a valid xml file containing lock identification details to import into the system. Export functionality will allow you to save a synchronized lock identification data file locally.

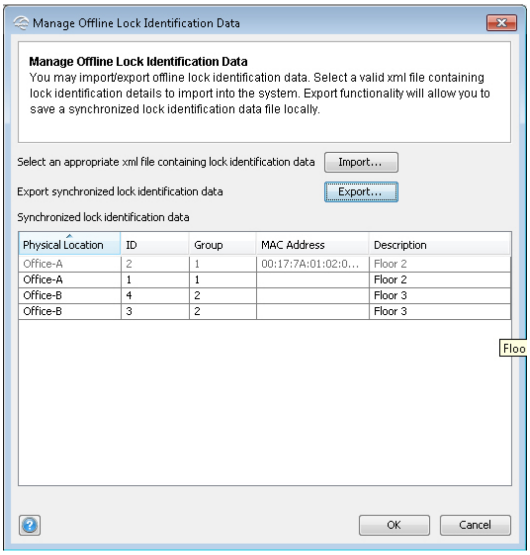
Physical Location	ID	Group	MAC Address	Description
Office-A	2	1	00:17:7A:01:02:0...	Floor 2
Office-A	1	1		Floor 2
Office-B	4	2		Floor 3
Office-B	3	2		Floor 3

Exporting lock identification data

1) Select *Installation - Offline - Manage Offline Lock Identification Data*.



2) Click the *Export...* button to save the installation performed.



Manage Offline Lock Identification Data

Manage Offline Lock Identification Data
You may import/export offline lock identification data. Select a valid xml file containing lock identification details to import into the system. Export functionality will allow you to save a synchronized lock identification data file locally.

Select an appropriate xml file containing lock identification data

Export synchronized lock identification data

Synchronized lock identification data

Physical Location	ID	Group	MAC Address	Description
Office-A	2	1	00:17:7A:01:02:0...	Floor 2
Office-A	1	1		Floor 2
Office-B	4	2		Floor 3
Office-B	3	2		Floor 3

Lock Identification Data XML format

Follow these guidelines when creating XML-file for defining lock identification data:

- Data file to be uploaded should contain list of lock identification data which will be imported into the system and can further be used to assign to different locks.
- File containing data should be in XML format.
- Data file should have xml extension(ex. door_data.xml).

Description of data

Tag/Attribute Name	Rules
<number>	A unique numeric value that is used to identify the lock on the site.
<groups>	The parent tag for the <group> tag, when specifying group/s for SOAA locks. This tag is only be used for SOAA locks and can contain up to 8 <group> items.
<group>	A numeric value representing the group that the lock belongs to. There can be multiple locks in a group.
<description>	A logical description for the lock.
<mac>	Represents the Mac address of the lock that has this identification data(number/group). An empty value for this tag will signify that this lock identification data can be assigned to a lock .

Sample data file content

See the F1-help in the Aperio Programming application for an example.

Lock Identification Data Import XSD

See the F1-help in the Aperio Programming application for XSD content.

Upgrade of lock firmware

This procedure is equal as for Aperio Online, see section "*Upgrade of communication hub/lock/sensor firmware" on page 68.*

6 Installation of Programming Application and USB Radio dongle firmware

Computer specifications

The Aperio Programming Application should be installed on a computer with the following specifications:

- Laptop
- 32/64-bit version of Windows 7, Windows 8, Vista or XP
- USB 2.0

Files needed for the installation

- Aperio Programming Application software version 2.6.6.X
- Encryption key file

The software is delivered from your local ASSA ABLOY company.

Installing the Programming Application

Follow these steps to install the Programming Application and the drivers necessary for installation of the Radio dongle:

1) Unpack the Aperio distribution file (i.e. Aperio_Online_PAP-x.y.z.zip/Aperio_Online_PAP_US-x.y.z.zip) in a temporary folder.

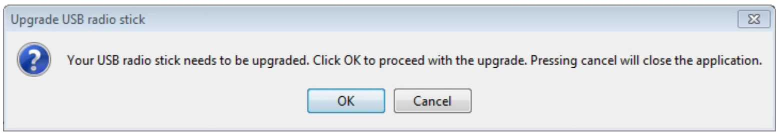
2) Run the setup-progapp-x.y.z.exe file.

Result: The Aperio Programming Application is installed and necessary drivers for the Radio dongle are copied to the computer.

USB Radio dongle firmware upgrade

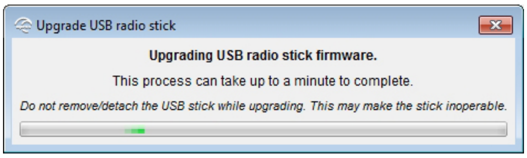
The USB radio dongle firmware version is checked both during installation of the Aperio Programming Application and when starting the application. An upgrade is automatically initiated if the USB radio dongle has an older firmware version than the current Programming application:

1) Click *OK* to perform firmware upgrade (or *Cancel* to close the application).


Upgrade USB radio stick

Your USB radio stick needs to be upgraded. Click OK to proceed with the upgrade. Pressing cancel will close the application.

2) The USB radio dongle is upgraded with the latest firmware.

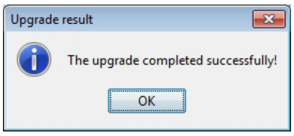

Upgrade USB radio stick

Upgrading USB radio stick firmware.

This process can take up to a minute to complete.

Do not remove/detach the USB stick while upgrading. This may make the stick inoperable.

3) Click OK after successful upgrade, to start the Programming application.


Upgrade result

The upgrade completed successfully!

7 Regulatory Information Regarding the Aperio USB Radio Dongle

Compliance

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada. Operation is subject to the following two conditions:

- this device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications made to this equipment not expressly approved by Tritech Technology AB may void the FCC authorization to operate this equipment.

According to FCC15.247

To comply with RF exposure compliance requirements, the device must not be co-located or operating in conjunction with any other antenna or transmitter.

According to FCC15.105 (b) Information to the user

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Security Statement

The following security measures are applicable to Aperio:

Authentication	3-pass mutual authentication (challenge-response protocol) based on AES128. Standard Aperio authentication scheme.
Confidentiality in communication	The communication is encrypted by a unique session key.
Confidentiality of information in the lock	Secret information such as encryption keys is never visible outside the protected flash of the micro controller.
Encryption key	Unique encryption key seed for each installation.
Database	The encrypted database in Programming Application is password protected. The computer must also be physically protected.
Applicable tests	AES and RNG tested according to NIST (National Institute of Standards and Technology) test vectors. http://csrc.nist.gov/groups/STM/cavp/documents/rng/RNGVS.pdf http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience

assaabloy.com/aperio

ASSA ABLOY

Contact

www.assaabloy.com/aperio

aperio™ Wireless lock technology